N-TRON
THE INDUSTRIAL NETWORK COMPANY

702-W and 702M12-W Industrial Ethernet Wireless Devices

User Manual & Installation Guide

702-W & 702M12-W Industrial Ethernet Wireless Device Installation Guide 3
Safety Warnings 5
Installation 7
Connecting the Unit 15
Web Management and Configuration 19
Configuration Guide 20
Navigation 20
System Info Page 21
System Information 22
Statistics Reporting 24
Extra Info 25
Tools 27
Link Setup Page 29
Basic Wireless Settings 29
Wireless Security 33
Network Page 36
Bridge Mode 37
Router Mode 38
Advanced Page 40
Advanced Wireless Settings 41
Acknowledgment Timeout 42
Antenna Alignment LED Thresholds 42
Wireless Traffic Shaping 43
Service Page 44
Ping WatchDog 44
SNMP Agent 46
NTP Client, Web Server, Telnet Server 47
System Config Page 48
Firmware 48
Host Name 49
Administrative Account 50
Interface Language 50
Configuration Management 50
Device Maintenance 50
Common Topology Scenarios 51
Scenario 1 – Basic Bridge 51
Scenario 2 – Encrypted Bridge 52
Scenario 3 – Controls Network 53
Scenario 4 – WDS Peering 54
Scenario 5 – Broadband Modem Wireless Router (W/ DHCP) 55
N-TRON Limited Warranty 60

702-W & 702M12-W Industrial Ethernet Wireless Device Installation Guide

The N-TRON 702-W Industrial Ethernet Wireless Device offers outstanding performance and ease of use. It is ideally suited for connecting wireless devices to a wired network and connecting two wired networks together where wires are not possible or practical to be installed.

PRODUCT FEATURES

- Full IEEE 802.3 Compliance
- One 10/100 BaseTX RJ-45 Port
- Three Antennas for 3x3 MIMO Operations
- Extended Environmental Specifications
- Autosensing 10/100BaseTX, Duplex, and MDIX
- Offers Spanning Tree Protocol
- Store & Forward Technology
- Rugged Din-Rail Enclosure (Bulk head mount for M12 version, Pole Mount Kit Available)
- Redundant Power Inputs (20-49 VDC)
- Full SNMP
- Web Browsing and N-View Monitoring
- IP65 Rated for protection against low pressure jets of water from any direction (M12 version)
- IP66 Rated for protection against high pressure jets of water from any direction (M12 version)
- IP67 Rated for protection against temporary immersion in water (M12 version)

WIRELESS COMPLIANCE

- IEEE 802.11a Compliant
- IEEE 802.11b Compliant
- IEEE 802.11g Compliant
- IEEE 802.11n draft Compliant

Copyright, © N-Tron Corp., 2009
820 S. University Blvd., Suite 4E
Mobile, AL 36609 USA

All rights reserved. Reproduction, adaptation, or translation without prior written permission from N-Tron Corp. is prohibited, except as allowed under copyright laws.

Ethernet is a registered trademark of Xerox Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks of their respective owners.

The information contained in this document is subject to change without notice. N-Tron Corp. makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. In no event shall N-Tron Corp. be liable for any incidental, special, indirect or consequential damages whatsoever included but not limited to lost profits arising out of errors or omissions in this manual or the information contained herein.

Warning

A well-trained technician is required to establish a wireless network safely. Do not perform any services on the unit unless qualified to do so.

Do not substitute unauthorized parts or make unauthorized modifications to the unit.

Do not operate the unit with the top cover removed, as this could create a shock or fire hazard.

Do not block the air vents on the sides or the top of the unit.

Do not operate the equipment in the presence of flammable gasses or fumes. Operating electrical equipment in such an environment constitutes a definite safety hazard.

Do not operate the equipment in a manner not specified by this manual.

Safety Warnings

GENERAL SAFETY WARNINGS

WARNING: If the equipment is used in a manner not specified by N-Tron Corp., the protection provided by the equipment may be impaired.

Contact Information

N-Tron Corp.
820 South University Blvd.
Suite 4E
Mobile, AL 36609
TEL: (251) 342-2164
FAX: (251) 342-6353
WEBSITE: www.n-tron.com
E-MAIL: N-TRON_Support@n-tron.com

ENVIRONMENTAL SAFETY

WARNING: Disconnect the power and allow to cool 5 minutes before touching.

WARNING: Explosion hazard; do not disconnect while circuit is live unless area is known to be non-hazardous.

ELECTRICAL SAFETY

Must be used with listed UL Class 2 Industrial Power Supply

WARNING: Disconnect the power cable before removing the top cover.

WARNING: Do not operate the unit with any cover removed.

WARNING: Properly ground the unit before connecting anything else to the unit. Units not properly grounded may result in a safety risk and could be hazardous and may void the warranty. See the grounding technique section of this user manual for proper ways to ground the unit.

WARNING: Do not work on equipment or cables during periods of lightning activity.

WARNING: Do not perform any services on the unit unless qualified to do so.

WARNING: Do not block the air vents.

WARNING: Observe proper DC Voltage polarity when installing power input cables. Reversing voltage polarity can cause permanent damage to the unit and void the warranty.

WARNING: The human body should be at least 20cm from these wireless devices during operation.

Please make sure the N-Tron Wireless Device package contains the following items:

1. 702-W or 702M12-W Wireless Device
2. Three Antennas
3. Product CD

Contact your carrier if any items are damaged.

Installation

Read the following warning before beginning the installation:

WARNING

Never install or work on electrical equipment or cabling during periods of lightning activity. Never connect or disconnect power when hazardous gasses are present.

Substitution of components may impair suitability for Division 2.

Always install antennas with adequate lightning and surge protection.

For IEEE 802.11b/g, 2.4GHz antennas are needed. For IEEE 802.11a, 5GHz antennas are needed.

Disconnect the power cable before removing any enclosure panel.

UNPACKING

Remove all the equipment from the packaging, and store the packaging in a safe place. File any damage claims with the carrier.

CLEANING

Clean only with a damp cloth.

INGRESS PROTECTION IP67

The classification of degrees of protection provided by the enclosures is defined by IEC 60529. Each rating is defined by specific tests.

The IP number is comprised of two numbers, the first referring to the protection against solid objects and the second against fluids. The higher the number, the better the device is protected against contact with moving parts and the harmful entry of various forms of moisture.

1st IP	Protection against ingress of solids	2nd IP	Protection against ingress of liquids
0	No protection	**0**	No protection
1	Protected against solid objects over 50mm e.g. hands, large tools.	**1**	Protected against vertically falling drops of water.
2	Protected against solid objects over 12mm e.g. hands, large tools.	**2**	Protected against direct sprays of water up to 15° from vertical.
3	Protected against solid objects over 2.5mm e.g. wire, small tools.	**3**	Protected against direct sprays of water up to 60° from vertical.
4	Protected against solid objects over 1.0mm e.g. wires.	**4**	Protected against water sprayed from any direction. Limited ingress permitted.
5	Limited protection against dust ingress (no harmful deposit)	**5**	Protected against low pressure water jets from any direction. Limited ingress permitted.
6	Totally protected against dust ingress.	**6**	Protected against high pressure water jets from any direction. Limited ingress permitted.
		7	Protected against temporary immersion between 15cm to 1m.
		8	Protected against long periods of immersion under pressure.

The 702M12-W Industrial Wireless Device is fully protected against dust and will remain sealed when immersed in water to a depth of 1 meter for 1 hour when all the ports are properly mated or sealed.

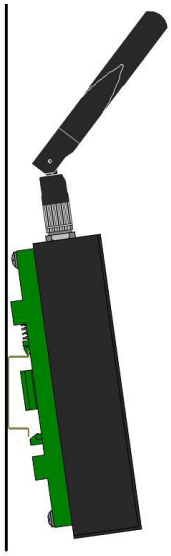
This IP67 cap seals off the LAN ports if unused to protect them from dirt, water, oil or any other contaminants which might be present in close proximity of the device.

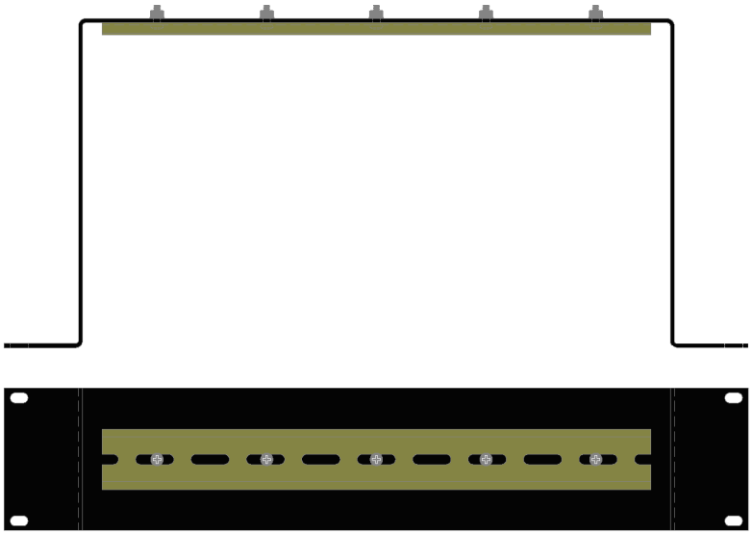
This IP67 cap seals off the Antenna ports if unused to protect them from dirt, water, oil or any other contaminants which might be present in close proximity of the device.

This IP67 cap seals off the Power port if unused to protect it from dirt, water, oil or any other contaminants which might be present in close proximity of the device.

702-W DIN RAIL MOUNTING

Install the unit on a standard 35mm Din-Rail. Recess the 702-W unit to allow at least 3” of horizontal clearance for copper cable bend radius.





DIN-Rail Mounting

To mount the unit to the 35mm DIN-Rail, place the top edge of the bracket on the back of the unit against the DIN-Rail's top edge at an upward angle. Then, rotate the unit downward and back against the DIN-Rail until it snaps into place. You may need to adjust the angle of the antennas depending on the amount of clearance available.

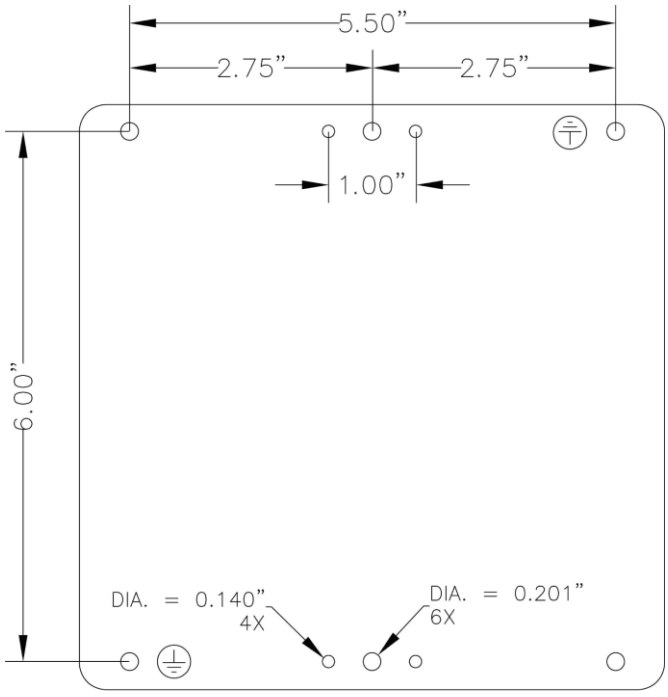
To remove the vertically mounted unit from 35mm DIN-Rail, carefully apply downward pressure on the unit. Then, rotate the unit upward and away from the 35mm DIN-Rail and lift up for removal.

19” Universal Rack Mounting

Most N-Tron™ products are designed to be mounted on industry standard 35mm DIN-Rail. However, DIN-Rail mounting may not be suitable for all applications. Our Universal Rack Mount Kit (P/N: **URMK**) may be used to mount the 702-W to standard 19" racks as an option.

702M12-W BULKHEAD MOUNTING

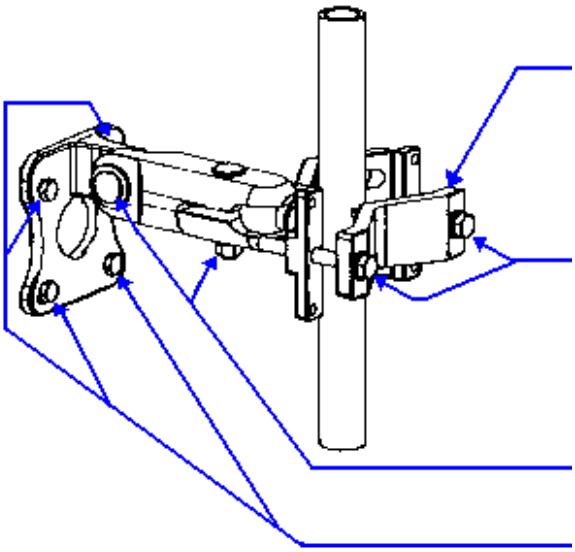
The following are the mechanical dimensions and drill hole placements to consider when mounting the 702M12-W Industrial Ethernet Switches:



702M12-W Back Plate

702M12-W POLE KIT MOUNTING

The 702M12-W can be mounted to a pole with N-Tron's 702M12 Pole Kit (P/N: 702M12-PK).

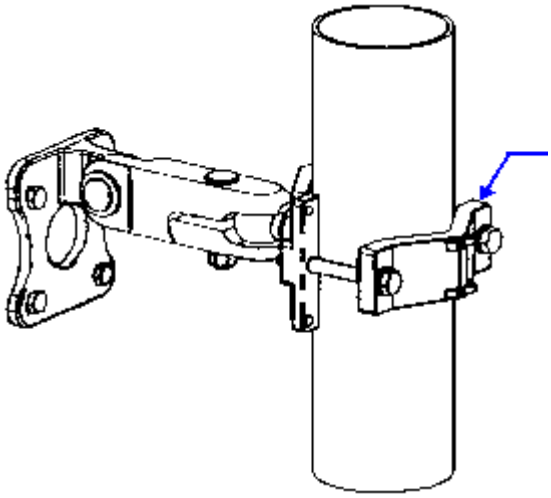


Bracket orientation for small (1" [25mm] dia.) pipe

2x Tighten bolts using 7-8 ft-lb of torque [9.49-10.85 N-m] (all pipe installations)

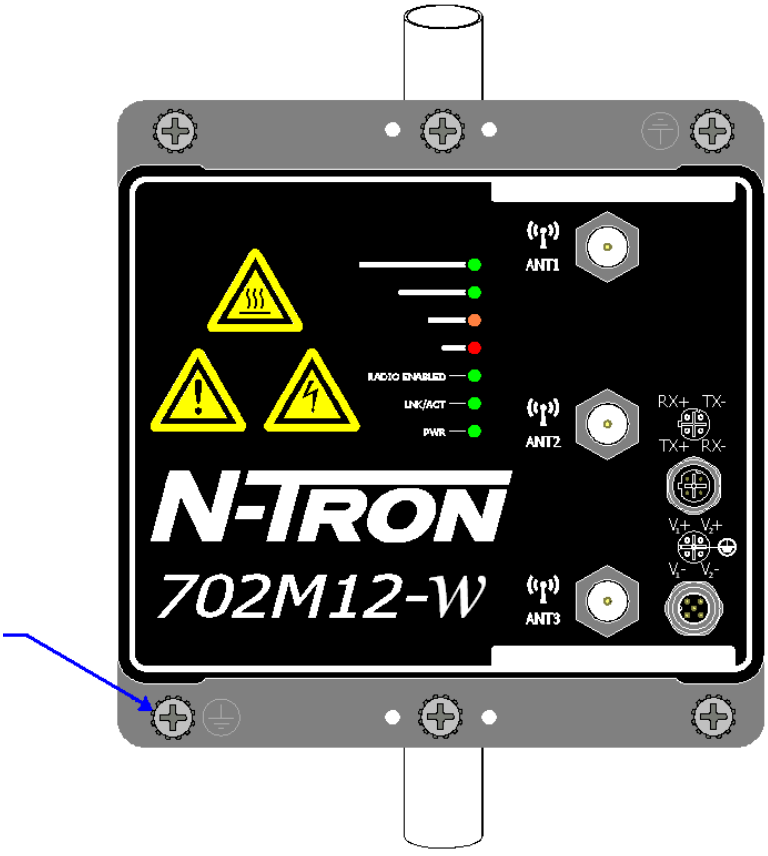
2x Tighten nuts using 10-11 ft-lb of torque [13.56-14.91 N-m] (all installations)

4x Tighten 0.250-20 bolts using 10-11 ft-lb of torque [13.56-14.91 N-m] (all installations)

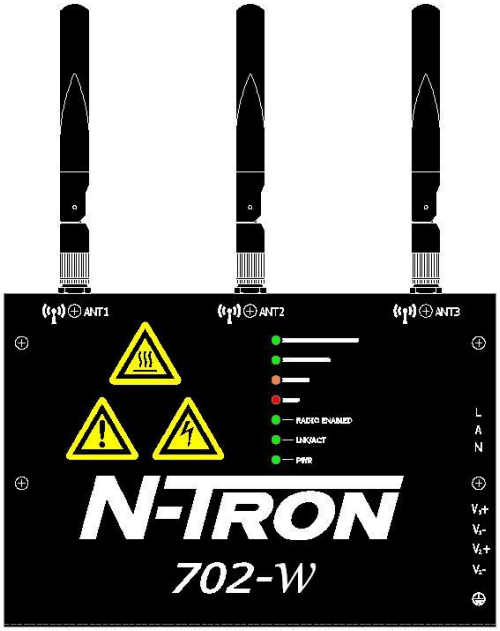


Bracket orientation for larger (up to 3" [76mm] dia.) pipe

6x Tighten #10-32 screws until split lock washers fully compress (all installations)



FRONT PANEL



From Top to Bottom (M12 only):

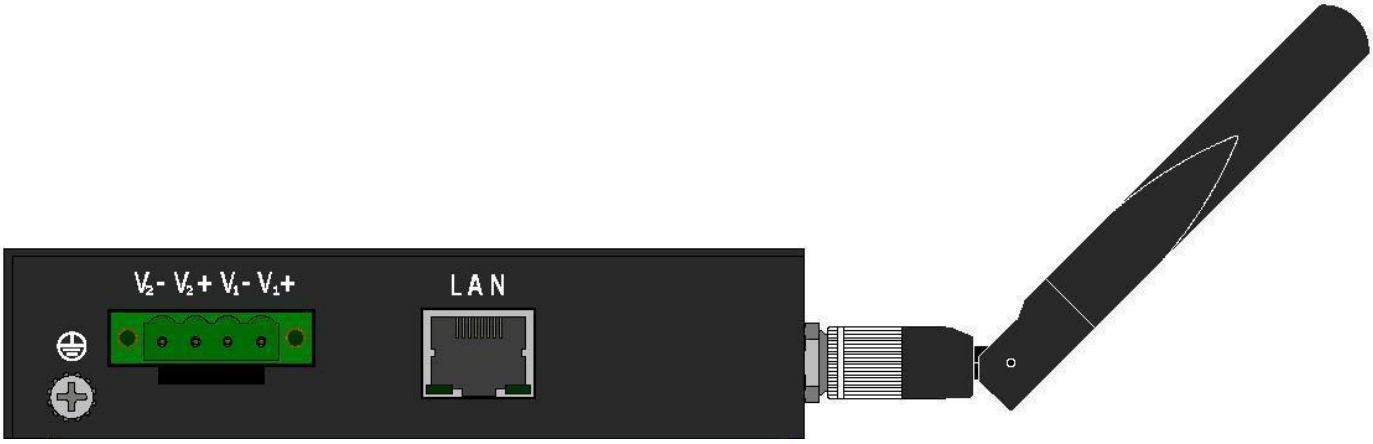
RJ45 Port Auto Sensing 10/100 Base-TX Connections with PoE Support

Power Port PWR LED lights when Power is supplied to the unit

LEDs: The table below describes the operating modes:

LED	Color	Description
	GREEN	Good Signal (user defined)
	ORANGE	Poor Signal (user defined)
	RED	Bad Signal (user defined)
Radio Enabled	GREEN	The radio interface is active
	OFF	The radio interface is off
LNK/ACT	GREEN	LAN Link is present
	FLASHING	Data is active over the ports
	OFF	No Link is present on the LAN port
PWR	GREEN	Power is applied
	OFF	No Power is applied

APPLYING POWER (702-W Side View)



- Unscrew & Remove the DC Voltage Input Plug from the Power Input Header
- Install the DC Power Cables into the Plug (observing polarity).
- Plug the Voltage Input Plug back into the Power Input Header.
- Tightening torque for the terminal block power plug is **0.5 Nm/0.368 Pound Foot.**
- Verify the Power LED stays ON (GREEN).

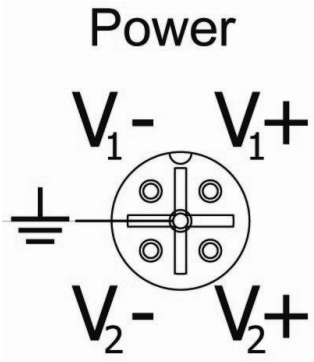
Notes:

- Only 1 power supply must be connected to power for minimal operation. For redundant power operation, V_1 and V_2 inputs must be connected to separate DC Voltage sources. This device will draw current from both sources simultaneously. Use 16-28 gauge wire when connecting to the power supply.
- The LAN port supports Power over Ethernet and can be used redundantly with the power input mentioned above.

Recommended 24V DC Power Supplies, similar to: N-Tron's P/N **NTPS-24-1.3:**

- Input AC 115/230V
- Output DC 24-28V
- Output Current 1.3A @ 24V
  1.0A @ 28V
- Power 72W
- 35 mm DIN-Rail Mountable
- Dimensions: 45X75X91 mm

APPLYING POWER (702M12-W)



The M12 A coded power connector is keyed, where the mating connection from the power supply can be made only when the male and female ends are lined up properly.
Verify the Power LED stays ON (GREEN).

Notes:

- Only 1 power supply must be connected to power for minimal operation. For redundant power operation, V_1 and V_2 inputs must be connected to separate DC Voltage sources. This device will draw current from both sources simultaneously. Use 16-28 gauge wire when connecting to the power supply.
- The LAN port supports Power over Ethernet and can be used redundantly with the power input mentioned above.

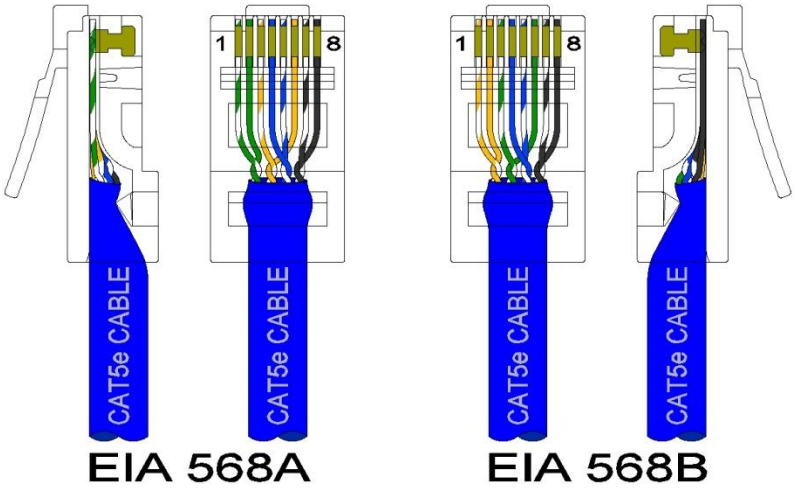
Recommended 24V DC Power Supplies, similar to: N-Tron's P/N **NTPS-24-1.3:** (NOTE: Not appropriate for use with M12, POE, and HV models.)

- Input AC 115/230V
- Output DC 24-28V
- Output Current 1.3A @ 24V
  1.0A @ 28V
- Power 72W
- 35 mm DIN-Rail Mountable
- Dimensions: 45X75X91 mm

Connecting the Unit

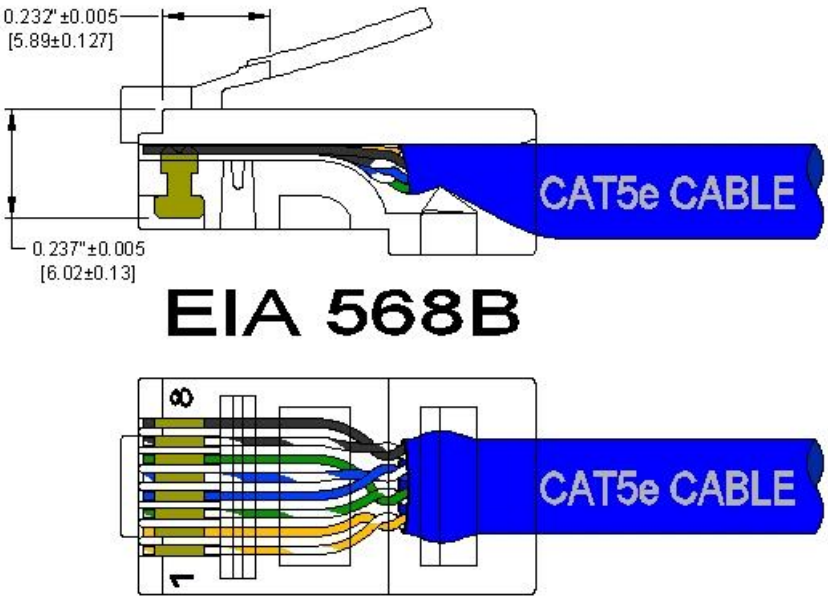
For the 10/100 Base-TX port, plug a Category 5E twisted pair cable into the RJ45 connector. Connect the other end to the far end station. Verify that the LNK/ACT LED is ON once the connection has been completed. Use a standard Category 5E straight through or crossover cable with a minimum length of one meter and a maximum length of 100 meters.

N-Tron recommends the use of pre-manufactured Cat5E cables to ensure the best performance. If this is not an option and users must terminate their own ends on the Cat5E cables; one of the two color coded standards shown to the right should be utilized. If a user does not follow one of these two color code standards then the performance and maximum cable distance will be reduced significantly, and may prevent the unit from establishing a link.



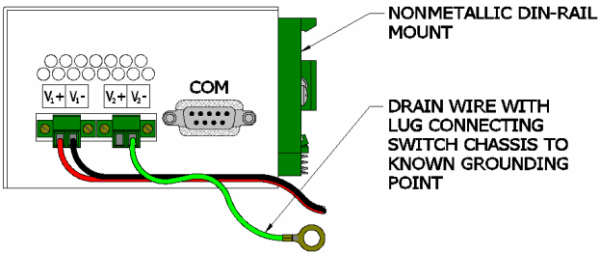
RJ45 CONNECTOR CRIMP SPECIFICATIONS

Please reference the illustration below for your Cat5 cable specifications:



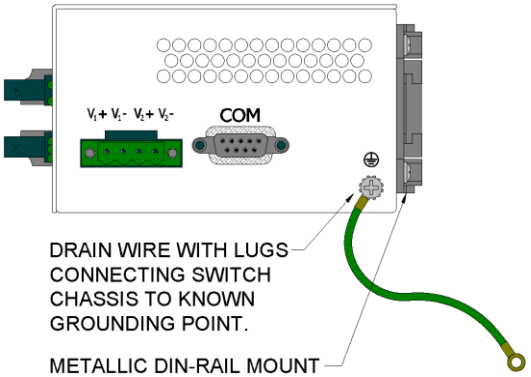
N-TRON SWITCH GROUNDING TECHNIQUES

The grounding philosophy of any control system is an integral part of the design. N-Tron switches are designed to be grounded, but the user has been given the flexibility to float the switch when required. The best noise immunity and emissions (i.e. CE) are obtained when the N-Tron switch chassis is connected to earth ground via a drain wire. Some N-Tron switches have metal din-rail brackets that can ground the switch if the din-rail is grounded. In some cases, N-Tron devices with metal brackets can be supplied with optional plastic brackets if isolation is required.



Both V- legs of the power input connector are connected to chassis internally on the PCB. Connecting a drain wire to earth ground from one of the V- terminal plugs as shown here will ground the switch and the chassis. The power leads from the power source should be limited to 3 meters or less in length.

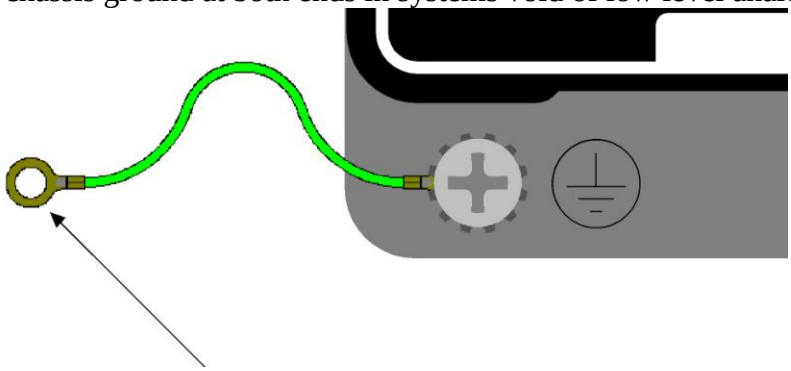
Alternatively, users can run a drain wire & lug from any of the Din-Rail screws or empty PEM nuts on the enclosure. When using an unused PEM nut to connect a ground lug via a machine screw, care should be taken to limit the penetration of the outer skin by less than 1/4 in. Failure to do so may cause irreversible damage to the internal components of the switch.



Note: Before applying power to the grounded switch, you must use a volt meter to verify there is no voltage difference between the power supply's negative output terminal and the device chassis grounding point.

If the use of shielded cables is required, it is generally recommended to only connect the shield at one end to prevent ground loops and interfere with low level signals (i.e. thermocouples, RTD, etc.). Cat5e cables manufactured to EIA-568A or 568B specifications are required for use with N-Tron devices.

In the event all Cat5e patch cable distances are small (i.e. All Ethernet devices are located the same local cabinet and/or referenced to the same earth ground), it is permissible to use fully shielded cables terminated to chassis ground at both ends in systems void of low level analog signals.



Drain wire with lug connecting switch chassis to known grounding point.

TROUBLESHOOTING

1. Make sure the PWR (Power LED) is ON.
2. Make sure you are supplying sufficient current for the version chosen. Note: The Inrush current will exceed the steady state current by ~ 2X.
3. Verify that Link LED is ON for the connected port.
4. Verify cabling used between stations.
5. Verify that cabling is Category 5E or greater for 100Mbit operation.

SUPPORT

Contact N-Tron Corp. at:
TEL: 251-342-2164
FAX: 251-342-6353
E-MAIL: N-TRON_Support@n-tron.com
WEB: www.n-tron.com

FCC STATEMENT

This product complies with Part 15 of the FCC Rules.
Operation is subject to the following conditions:
(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

ANTENNA STATEMENT

The regulatory domain this equipment is installed in has a legal limit for the equivalent isotropic radiated power (EIRP) that is determined by the output power and the antenna gain. It is the installer's responsibility to make sure this rule is not violated. All equipment should be professionally installed. After proper installation the device should be properly protected to ensure regulatory compliance.

FCC sets the maximum gain for the following antenna types for the 702-W Radios;

2.4GHz Omni-Directional	5dBi
2.4GHz Panel Directional	17dBi
5.8GHz Panel Directional	21dBi
5.8GHz Parabolic Dish	32dBi

NOTE: External Antennas should be installed and operated with a minimum distance between the radiator and any person or operator. This distance is determined by the regulatory domain the equipment is installed in and should be calculated by the installer at the time of installation to ensure regulatory compliance and the safety of operators around the radiator.

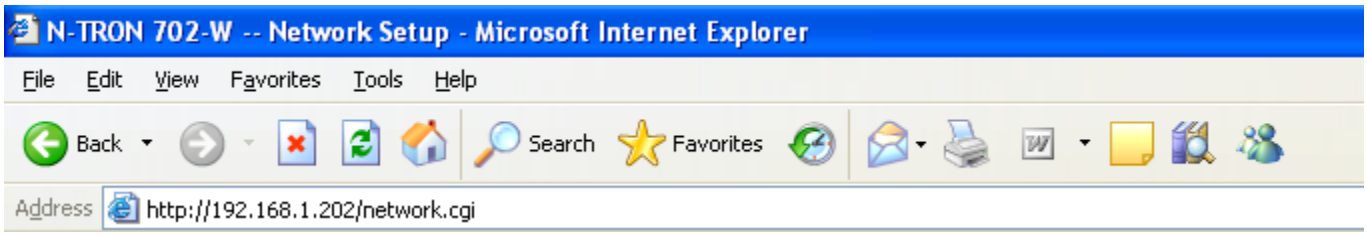
INDUSTRY CANADA

This Class A digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations (ICES-003). Operation is subject to the following two conditions; (1) this device digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations. Operation is subject to the following two conditions; (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Cet appareillage numérique de la classe A répond à toutes les exigences de l'interférence canadienne causant des règlements d'équipement (NMB-003). L'opération est sujette aux deux conditions suivantes: (1) ce dispositif peut ne pas causer l'interférence nocive, et (2) ce dispositif doit accepter n'importe quelle interférence reçue, y compris l'interférence qui peut causer l'opération peu désirée.

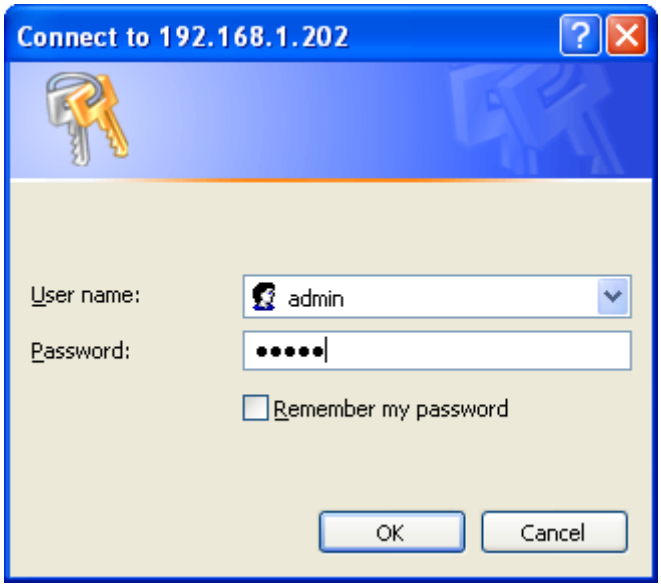
Web Management and Configuration

Enter the device's IP address in any web browser and login to the web management feature of the 702-W.



Default:

IP Address: ***192.168.1.202***
User Name: ***admin***
Password: ***admin***



Configuration Guide

This guide presents the detailed description of the N-TRON 702-W operating system which is integrated into the N-TRON 702W.

N-TRON 702-W Quick Setup Guide describes the configuration steps for the subscriber station (wireless client - bridge).

All the configuration settings accessible via web management interface are described in this document.

Device support the following operating modes for 802.11 a/b/g/n:

- Station (Client)
- Station WDS
- Access Point
- Access Point WDS / Peer

All the devices support the following network modes:

- Transparent bridge- layer 2
- Router- layer 3

Navigation

Configuration Management Menu

Each of the web management pages (listed below) contains parameters that affect a specific aspect of the device:

System Info page displays current status of the device and statistical information. There are useful network administration and monitoring tools available on the Main page (i.e. speed test utility, site survey functionality in AP mode).

Link Setup page contains the controls for the wireless network configuration, covering basic wireless settings which define device operating modes, associating details, and data security options.

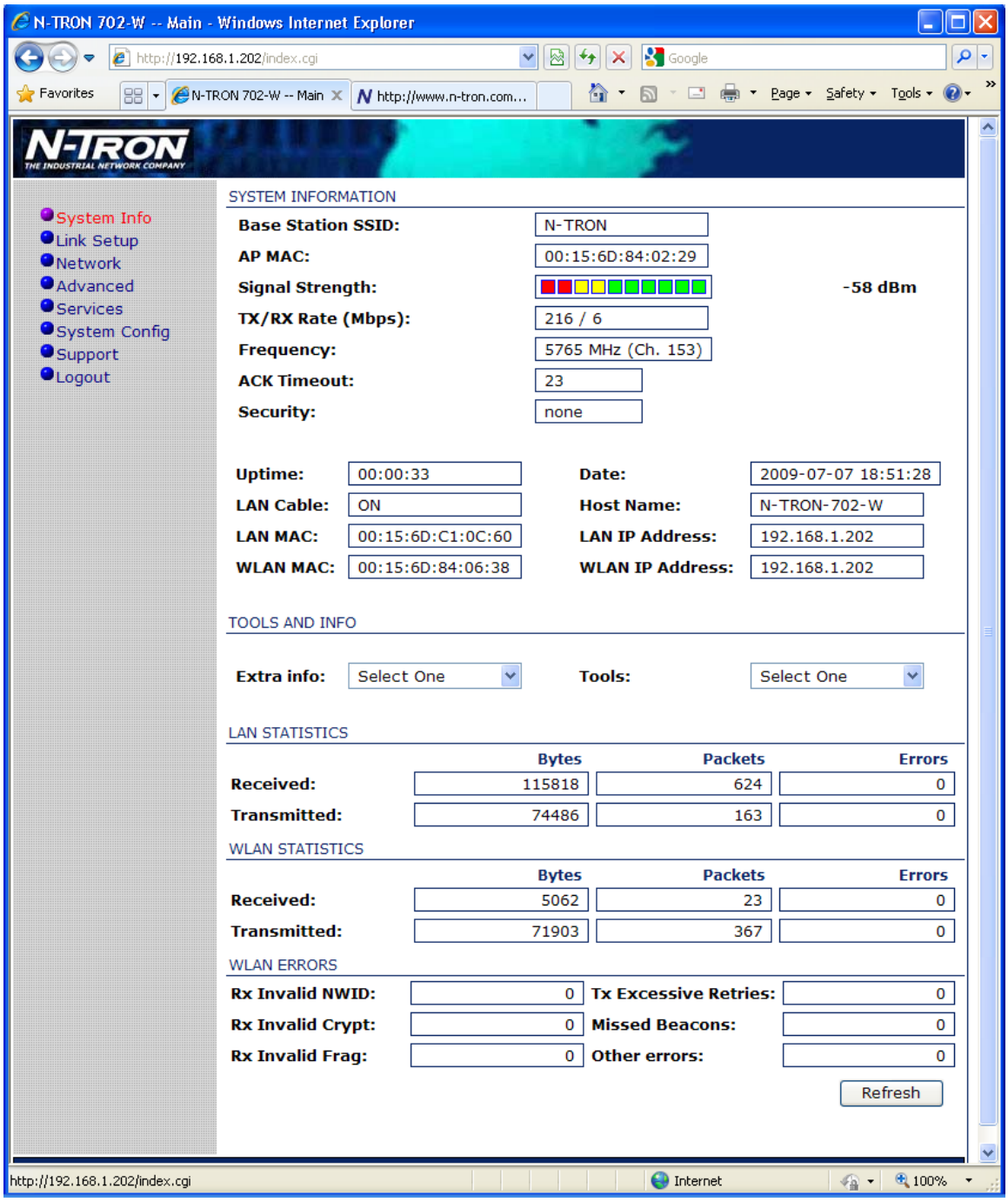
Network page covers the configuration network operating modes, IP settings, packet filtering routines and network services (i.e. DHCP Server).

Advanced page settings are dedicated for more precise wireless interface control, including RTS, fragmentation, aggregation, traffic shaping and QoS settings.

Services page covers the configuration of system management services (i.e. SNMP, NTP, Ping Watchdog, Web, Telnet, SSH, Log).

System Config page contains controls for system maintenance routines, administrator account management, Host Name, firmware and configuration backup.

System Info Page



The **System Info** Page displays a summary of link status information, basic configuration settings of the device (operating mode, network settings), and traffic statistics of all the interfaces.

Network administration and monitoring utilities such as antenna alignment, ping test, and speed test tools are accessible via *System Info* page also.

System Information

Base Station SSID: The Name of the 802.11 Service Set (established by the Host Access Point) the device is connected to:

While operating in Station mode, displays the BSSID of the Access Point where the device has associated. While operating in Access Point mode, displays the BSSID of the wireless device itself.

AP MAC: displays the MAC address of the Access Point where the device has associated while operating in Station mode. MAC (Media Access Control) is the unique HW identifier on each 802.11 radio.

Signal Strength: displays the received wireless signal level (client-side) while operating in Station mode. The represented value coincides with the graphical bar. Use the antenna alignment tool to adjust the device antenna to improve the link with other wireless devices. The antenna of the wireless client has to be adjusted to get the maximum signal strength. Signal Strength is measured in dBm (the Decibels referenced to 1 milliwatt). The conversion is defined as dBm=10log10(P/1mW). So, 0dBm would be 1mW and –72dBm would be .0000006mW. A signal strength of –85dBm or better is recommended for stable links.

Antenna Alignment: This utility allows the user to optimize the antenna direction for maximum link signal. More information is provided in the *Tools* sub-section.

TX Rate and RX Rate: displays the current 802.11 data transmission (TX) and data reception (RX) rate while operating in *Station* mode. Data rates at 1,2,5.5,11Mbps (802.11b) and 6,9,12,18,24,36,48,54Mbps (802.11) are possible. Typically, the higher the signal, the higher the data rate, and consequently the higher the throughput. For maximum throughput (54Mbps), typically a –70dBm or better signal is required.

Frequency: This is the operating frequency and channel of the 802.11 Service Set (hosted by AP) the client is connected to. Device uses this frequency to transmit and receive data. For 802.11Na operation, the range of available frequencies are 5.745-5.825Ghz and for 802.11b/g/n operation, 2412-2472 MHz. However, the specific frequencies that can be used will vary depending on local country regulations.

ACK Timeout: displays the current ACK Timeout value, which is set on the device manually or adjusted automatically. The ACK Timeout (Acknowledgment Timeout) specifies how long the N-TRON 702-W device should wait for an acknowledgment from a partner device confirming packet reception before concluding the packet must have been in error and requires resending. ACK Timeout is a very important outdoor wireless performance parameter. The ACK timeout is in microseconds. More information is provided in the *Advanced* settings section.

Security: This is the current security setting. More information is provided in the *Link Setup* section.

Uptime: This is the running total of time the device has been running since last power up (hard-reboot) or software upgrade. The time is expressed in days, hours, minutes and seconds.

Date: indicates the current system date and time, expressed in the form “year-month-day hours:minutes:seconds”. System date and time can be retrieved from the Internet services using NTP (Network Time Protocol).

LAN cable: displays the current status of the Ethernet port connection. This can alert operator/user/technician that the LAN cable is plugged into the device and there is an active Ethernet connection.

Host Name: displays the customizable name (ID) of the device as it will appear in popular Router Operating Systems registration screens.

LAN MAC: displays the MAC address of the N-TRON 702-W device LAN (Ethernet) interface.

LAN IP Address: displays the current IP address of the LAN (Ethernet) interface.

WLAN MAC: displays the MAC address of the N-TRON 702-W device WLAN (Wireless) interface.

WLAN IP Address: displays the current IP address of the WLAN (Wireless) interface.

Note: *LAN IP Address* and *WLAN IP Address* displays the same value - current IP address of the virtual *bridge* interface, while the device is operating in *Bridge* mode.

Statistics Reporting

LAN Statistics: section displays the detailed receive and transmit statistics (*Bytes, Packets, Errors*) of the *LAN* (Ethernet) interface. These statistics represent the total amount of data and packets transferred between devices through the Ethernet interface from either direction.

Both unicast IP traffic (conversations between two hosts using HTTP, SMTP, SSH and other protocols) and broadcast traffic (while addressing all hosts in a given network range with a single destination IP address) is accounted.

As long as there is some network traffic being generated or passed through the *LAN* interface, Received and Transmitted *Bytes* and *Packets* value will continue to increase. The *Errors* value represents the total number of transmitted and received packets for which an error occurred.

WLAN Statistics: section displays the detailed receive and transmit statistics (*Bytes, Packets, Errors*) of the *wireless* interface.

These statistics represent the total amount of unicast and broadcast IP data transferred between devices through the *wireless* interface from either direction.

As long as there is some network traffic being generated or passed through the *wireless* interface, Received and Transmitted Bytes, Packets, and Errors (if any); statistic counters will continue to increase.

WLAN Errors: section displays the counters of 802.11 specific errors which were registered on *wireless* interface:

> **Rx invalid NWID** value represents the number of packets received with a different NWID or ESSID - packets which were destined for another access point. It can help detect configuration problems or identify the adjacent wireless network existence on the same frequency.
> **Rx Invalid Crypt** value represents the number of transmitted and received packets which were encrypted with the wrong encryption key and failed the decryption routines. It can be used to detect invalid *wireless security* settings.
> **Rx Invalid Frag** value represents the number of packets missed during transmission and reception. These packets were dropped due to re-assembling failure as some link layer fragments of the packet were lost.
> **Tx Excessive Retries** value represents the number of packets which failed to be delivered to the destination. Undelivered packets are retransmitted a number of times before an error occurs.
> **Missed beacons** value represents the number of beacons (management packets sent at regular intervals by the Access Point) which were missed by the client. This indicates that the client is out of range.
> **Other errors** value represents the total number of transmitted and received packets that were lost or discarded for other reasons.

The content of the *System Info* page can be updated by using the **Refresh** button.

Extra Info

Extra Info: displays the current device usage statistics and status of the system components in a pop-up window.

- **Show Stations**: selection lists the stations which are connected to the device while operating in Access Point mode.

  Statistics for all stations (**RSSI**, **Tx Rate**, **Rx Rate** and **Idle** time) can be updated using the **Reload** button.

  More statistics (**Station Uptime**, **Negotiated Rates**, **Static** WDS Flag, **Tx/Rx Frames**, **Tx/Rx Bytes**) can be retrieved while clicking on the "+" button near MAC address of the each Station entry.

  RSSI - **Received Signal Strength Indication** (**RSSI**) is a measurement of the power present in a received radio signal.

- **Show ARP Table**: selection lists all entries of the ARP (Address Resolution Protocol) table currently recorded on the device.

  The list can be updated using the **Reload** button.

  ARP is used to associate each IP address to the unique hardware address (MAC) of the devices. It is important to have unique IP addresses for each MAC or there will be ambiguous routes in the network.

- **Show Throughput** selection continuously represents the current data traffic on the LAN and WLAN interfaces in both graphical and numerical form.

  The statistics is updated automatically and can be updated using the **Reload** button.

- **Show Log** selection displays system log information

- **Show Bridge Table**: selection lists all entries in the system bridge table, while the device is operating in *Bridge* mode.

The list can be updated using the **Reload** button.

Bridge table shows to which *bridge* port the particular station is associated to - in other words from which *interface* (Ethernet or wireless) the network device (defined by *MAC address*) is reachable to the N-TRON 702-W system while forwarding the packets to that port only (thus saving a lot of redundant copies and transmits).

Aging timer shows aging time for each address entry (in seconds) - after particular time out, not having seen a packet coming from a certain address, the bridge will delete that address from the Bridge Table.

- **Show Routes**: selection lists all of the entries in the system routing table, while the device is operating in Router mode.

The list can be updated using the **Reload** button.
N-TRON 702-W examines the *destination IP address* of each data packet traveling through the system and chooses the appropriate interface for packet forwarding. The system choice depends on static routing rules – entries, which are registered in the system routing table. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of all the N-TRON 702-W interfaces.
N-TRON 702-W IP configuration description is provided in the *Link Setup* section.

- **Show Firewall** selection lists active firewall entries in the *FIREWALL chain* of the standard ebtables *filter table*, while the device is operating in *Bridge* mode.

  ATH0 - Wireless Interface
  ETH0 - Lan/Wired Interface
  BR0 - Bridge Interface of ATH and ETH when in bridge mode
  PPP - Interface when utilizing a PPPOE connection

  The list can be updated using the **Reload** button.
  Active firewall entries in the *FIREWALL chain* of the standard iptables *filter table* are listed if the device is operating in *Router* mode.

  IP and MAC level access control and packet filtering in N-TRON 702-W is implemented using iptables (routing) and ebtables (bridging) firewall which protects the resources of a private network from outside threats by preventing unauthorized access and filtering specified types of network communication.
  More information is provided in the *Link Setup* section.

- **Show Port Forward** selection shows ports forwarded to internal devices through NAT in router mode

- **Show DHCP Leases** selection shows the current status of the leased IP addresses by the device's DHCP server.

  Interface name shows from which device interface DHCP client which has specified *MAC Address* is connected.

  Remaining Lease time shows for how long the leased *IP address* will be valid and reserved for a particular DHCP client.

  The list can be updated using the **Reload** button.

Tools

Tools: provides network utilities in a pop-up window:

- **Align Antenna:** This utility allows the installer to point and optimize the antenna in the direction of maximum link signal. The "RSSI Range" slider bar allows the range of the meter to be either increased or reduced. If the range is reduced, the color change will be more sensitive to signal fluctuations.

  Click the **Align Antenna** button and the new pop-up window with signal strength indicator will appear.

  RSSI Range slider can be used to change an offset of the maximum indicator value. Window reloads every second displaying current value of the signal strength.

- **Speed Test**: This utility allows for testing the connection speed to and from any reachable IP address on the N-TRON 702-W device network. It should be used for the preliminary throughput estimation between two network devices. If both devices are powered by N-TRON 702-W, the estimation is more precise, otherwise only rough estimation is provided while using ICMP packet exchange routines.

  Access credentials (administrator username - **User** and **Password**) of the remote system should be provided for the communication between two N-TRON 702-W powered devices.
  Remote system IP can be selected from the list which is generated automatically (*Select destination IP*) or can be *specified manually*.
  There are 4 options available for the traffic *direction* while estimating throughput:
    - Estimate the incoming maximal throughput (Rx) while selecting receive option;
    - Estimate the outgoing maximal throughput (Tx) while selecting transmit option;
    - First estimate the incoming (Rx) and afterwards the outgoing (Tx) maximal throughput while selecting both option;
    - Estimate the incoming (Rx) and the outgoing (Tx) maximal throughput at the same time while selecting duplex option.

  Test *Duration* and *Data amount* values can be specified while defining the test execution time criteria. If both criteria are specified, the test will stop after any of the criteria is met.

  The test is started using the **Run Test** button.

- **Ping**: This utility will ping other devices on the network directly from the N-TRON 702-W device.

  Ping utility should be used for the preliminary link quality and packet latency estimation between two network devices using the ICMP packets. Remote system IP can be selected from the list which is generated automatically (*Select destination IP*) or can be *specified manually*. The size of the ICMP packets can be specified in the *Packet size* field. Estimation is done after the number of ICMP packets (specified in *Packet count* field) is transmitted/received. Packet loss statistics and latency time evaluation is provided after the test is completed.

  The test is started using the **Start** button.

- **TraceRoute**: Allows tracing the hops from the N-TRON 702-W device to a selected outgoing IP address. It should be used for finding the route taken by ICMP packets across the network to the *Destination host*.

  Resolution of the IP addresses (symbolically rather than numerically) can be enabled by selecting the **Resolve IP address** option.

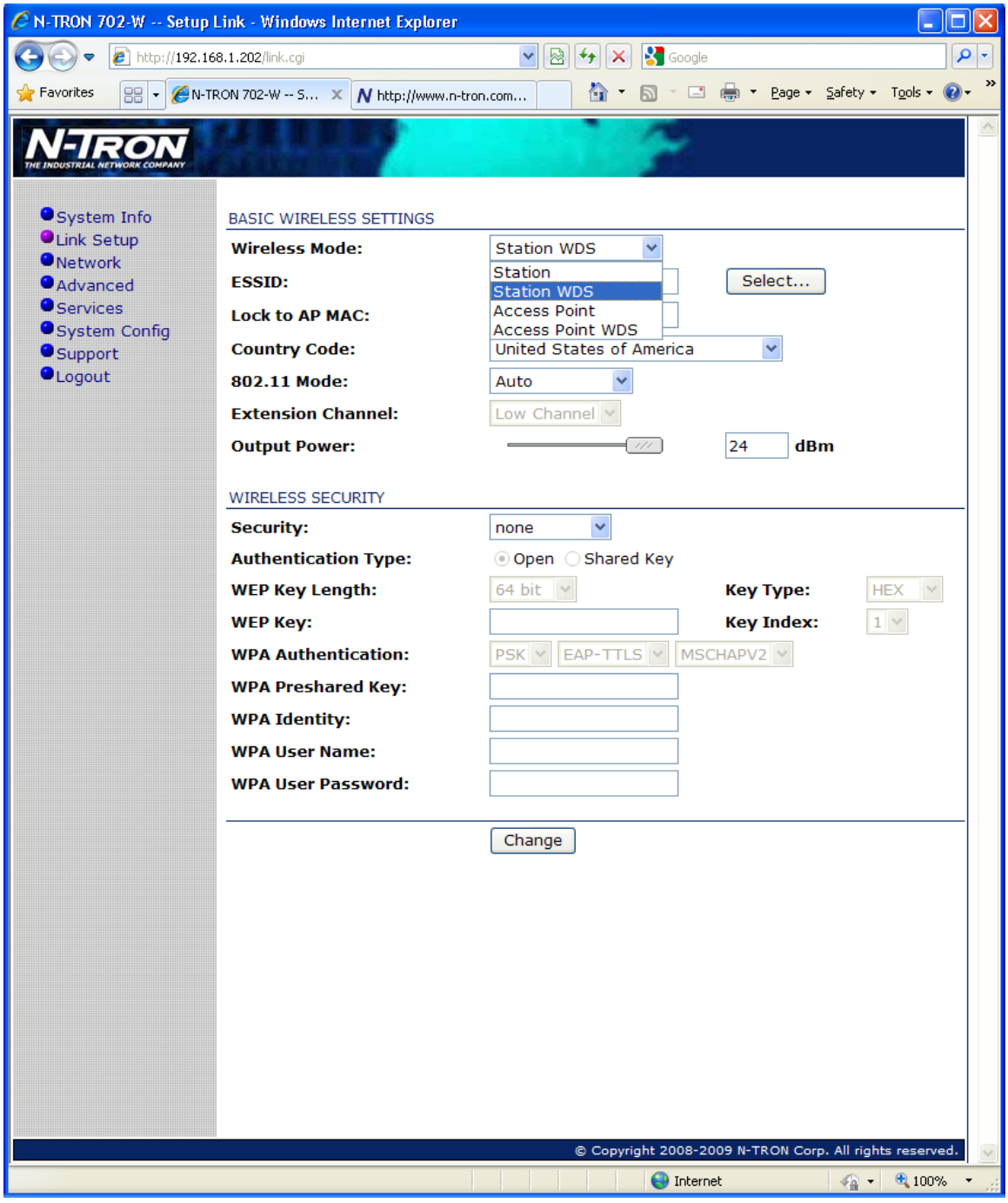
  The test is started using the *Start* button.

- **Site Survey**: utility will search for wireless networks in range on all supported channels while the device is operating as an *Access Point* or a *Station*. In Station mode the channel list can be modified. Refer to the section Link Setup for the details on channel list customization.

  Site Survey will report *MAC Address, SSID, Encryption* type (if any), *Signal Strength, Frequency* and the wireless *channel* used for each Access Point found.

  The Site Survey can be updated using the **Scan** button.

Link Setup Page



The Link Setup Page contains everything needed by the operator to setup the wireless part of the link. This includes regulatory requirements, channel and frequency settings, device mode, data rates, and wireless security.

Basic Wireless Settings

The general wireless settings, such as wireless device BSSID, country code, output power, 802.11 mode and data rates can be configured in this section.

Wireless Mode: specify the operating mode of the device. The mode depends on the network topology requirements. There are 4 operating modes supported in N-TRON 702-W software:

1. *Station*: This is a client mode, which can connect to an AP.
   It is common for bridging applications when one non-wireless devices needs to be connected to an AP. In *Station* mode the device acts as the Subscriber Station while connecting to the primary Access Point which is defined by the SSID and forwarding all the traffic to/from the network device connected to the Ethernet interface.
   More specifically *Station* mode uses *arpnat* technology which may result lack of transparency while passing-through *broadcast* packets in *bridge* mode.

2. *Station WDS*: WDS stands for Wireless Distribution System. Station WDS should be used while connecting to an Access Point which is operating in WDS mode.
   ***Station WDS mode enables packet forwarding at layer 2 level.**
   The benefit of *Station WDS* is improved performance and faster throughput. *Station WDS - Bridge* mode is fully transparent for all Layer2 protocols.
   Refer to the Network Settings section for detailed Bridge network mode configuration information.

3. *Access Point*: This is an 802.11 Access Point mode.

4. *Access Point WDS*: This is an 802.11 Access Point which allows **layer 2 bridging** with Station WDS devices using the WDS protocol.
   WDS allows you to bridge wireless traffic between devices which are operating in *Access Point* mode. Access Point is usually connected to a wired network (Ethernet LAN) allowing wireless connection to the wired network. By connecting Access Points to one another in an Extended Service Set using the WDS, distant Ethernets can be bridged into a single LAN.

It is very important that network loops not be created with either WDS bridges or combinations of wired (Ethernet) connections and WDS bridges. Tree or Star shape network topologies should be used in all WDS configurations (i.e. if AP2 and AP3 are specified as the WDS peers of AP1, AP2 should not be specified as the WDS peer of AP3 and AP3 should not be specified as the WDS peer of AP2 in any case). Mesh and Ring network topologies are not supported by WDS and should be avoided.

Note: *Station WDS* and *AP WDS* mode uses the WDS protocol which is not defined as the standard thus compatibility issues between equipment from different vendors may arise.

WDS Peers: WDS Stations and/or WDS Access Points connected to the 702-W Access Point should be specified in this list in order to create a wireless network infrastructure - Wireless Distribution System (applicable for AP WDS mode only).

Enter the MAC address of the paired WDS device in the WDS Peer entry field. One MAC address should be specified for Point-to-Point connections. Up to six WDS Peers can be specified for Point-to-Multi-Point connections.

Note: Access Point operating in WDS mode and all WDS Peers must operate on the same frequency *channel* and use the same *channel spectrum width*. Only WEP encryption is supported between WDS Peers.

SSID: Service Set Identifier used to identify your 802.11 wireless LAN should be specified while operating in *Access Point* mode. All client devices within range will receive broadcast messages from the access point advertising this SSID. **ESSID**: specify the ESSID of the Access Point which the N-TRON 702-W should associate to while operating in *Station* or *Station WDS* mode. There can be several Access Points with the same ESSID. If the ESSID is set to "Any" the *station* will connect to any available AP.

The list of available Access Points can be retrieved using the *Select* button, which activates the *Site Survey* tool with the AP selection functionality. Site Survey will search for the available wireless networks in range on all supported channels and will allow you to select one for association. In case the selected network uses encryption, you'll need to set security parameters in the wireless security section. Select the Access Point from the list and click the **Select** button for association.

Click **Scan** button to refresh the list of available wireless networks.

The **Close this window** button closes Site Survey tool window.

Site Survey channel scan list can be modified using the *Channel Scan List* control.

Channel Scan List: This will confine scanning only to the frequencies selected (applicable for Station and Station WDS modes only). The benefits of this are faster scanning as well as filtering out unwanted AP's. The Site Survey tool will look for the Access Points in the selected channels only.

Channel list management for the selected IEEE 802.11 mode and specified Channel Spectrum Width can be enabled by selecting the **Enabled** option. There are two ways to set the Channel Scan List - enumerating the required channels (separated by comma) in the input field or using the selection window which is activated using the **Edit** button.

Hide SSID control will disable advertising the SSID of the access point in broadcast messages to wireless stations. Unselected control will make SSID visible during network scans on the wireless stations. Control is available while operating in *Access Point* mode only.

Lock to AP MAC: This allows the station to always maintain connection to a specific AP with a specific MAC (applicable for Station and Station WDS modes only). This is useful as sometimes there can be a few identically named SSID's (AP's) with different MAC addresses. With AP lock on, the station will lock to the MAC address and not roam between several Access Points with the same ESSID.

Country Code: Different countries will have different power levels and possible frequency selections. To ensure device operation follows regulatory compliance rules, please make sure to select your correct country where device will be used. The channel list, output power limits, IEEE 802.11 and Channel Spectrum Width modes will be tuned according to the regulations of the selected country.

IEEE 802.11 Mode: This is the radio standard used for operation of your N-TRON 702-W powered device. 802.11b is an older 2.4GHz mode while the 802.11g (2.4GHz) and 802.11a (5GHz) are newer standards based on faster Orthogonal Frequency Division Multiplexing (OFDM) modulation.

702-W supported IEEE 802.11 modes:

802.11NG – 20MHz
802.11NG – 40MHz
802.11NA – 20MHz

802.11NA - 40MHz

Channel Spectrum Width: This is the spectral width of the radio channel. Supported wireless channel spectrum widths:

20MHz – is the standard channel spectrum width (selected by default).
40MHz – the widest channel spectrum width required to connect to an 802.11 a/g/n network which supports MIMO.

Reducing spectral width provides 2 benefits and 1 drawback.

Benefits:

- It will increase the amount of non-overlapping channels. This can allow networks to scale better.
- It will increase the PSD (Power Spectral Density) of the channel and enable the link distance to be increased.

Drawbacks:

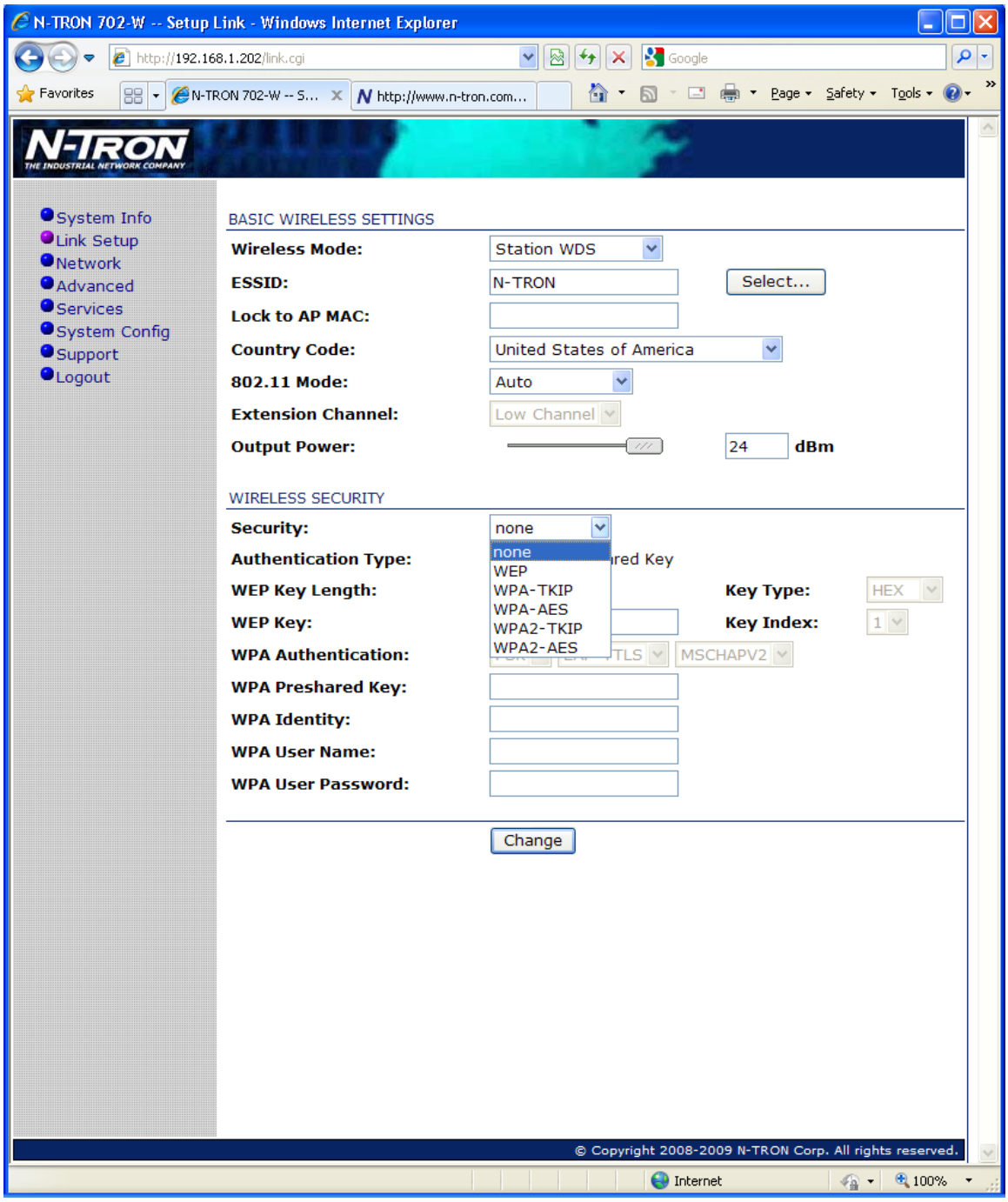
- It will reduce throughput proportional to the channel size reduction. So just as turbo mode (40MHz) increases possible speeds by 2x, half spectrum channel (10MHz), will decrease possible speeds by 2x.

Output Power: This will configure the maximum average transmit output power (in dBm) of the wireless device. The output power at which the wireless module transmits data can be specified using the slider. When entering the output power value manually, the slider position will change according to the entered value. The transmit power level that is actually used is limited to the maximum value allowed by your country's regulatory agency.

Data Rate: This defines the data rate (in Mbps) at which the device should transmit wireless packets. If the **Auto** check box is enabled, then the *rate algorithm* will select the best data rate depending on the link quality conditions. If a data rate below 54Mbps is selected while the *Auto* rate selection is enabled, then the selected data rate will become the maximum data rate that can be used. Use *Auto* option if you are having trouble getting connected or losing data at a higher rate. In this case the lower data rates will be used by the device automatically.

Refer to the section *Advanced Wireless Settings* for detailed information about *rate algorithms*.

Wireless Security



This section enables you to set parameters that control how the subscriber station associates to a wireless device and encrypts/decrypts data.

Station Wireless Security Settings

Choose the security method according to the Access Point security policy. The subscriber station should be authorized by the Access Point in order to get access to the network and all the user data transferred between subscriber station and Access Point will be encrypted if the wireless security methods are used.

Security: N-TRON 702-W supports all popular 802.11 security options such as WEP, WPA, and WPA2. Select the security mode of your wireless network:

> **WPA** – enable WPA™ security mode. Wi-Fi Protected Access - WPA™ (IEEE 802.11i/D3.0) and WPA2™ (IEEE 802.11i) with pre-shared key management protocol offers improved security methods as they are new protocols that were created under the 802.11i standard to address weaknesses in the WEP approach.

WPA™ and *WPA2*™ support the following ciphers for data encryption:

> *TKIP* - Temporal Key Integrity Protocol which uses the RC4 encryption algorithm.
> *CCMP* - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol which uses the Advanced Encryption Standard (AES) algorithm.

The device will use the strongest cipher (CCMP) in Station and Access Point wireless mode by default. If CCMP is not supported on the other side of the link, the TKIP encryption will be used. For instance, when the device acts as an Access Point with WPA security enabled and at least one wireless station (without CCMP support) is connected to it.

> *WPA-AES* – enable WPA™ security mode with AES support only.
> *WPA2-AES* – enable WPA2™ security mode with AES support only.

WPA Authentication: Choose between PSK and EAP.

PSK – Pre-shared Key – Type in the key to be shared for authentication between the AP and Station.

> *EAP* – Extensible Authentication Protocol – Uses TTLS and MSCHAPv2 for Authentication against an EAP authentication server
> WPA Identity – For EAP only - The identity of the EAP server
> WPA Username – EAP Only - Username
> WPA Password – EAP Only - Password

WPA Authentication: one of the following WPA™ key selection methods should be specified if WPA™ or WPA2™ security method is used (applicable for *Station* and *Station WDS* modes only):

> *PSK* – WPA™ or WPA2™ with Pre-shared Key method (selected by default).
> *EAP* – WPA™ or WPA2™ with EAP (Extensible Authentication Protocol) IEEE 802.1x authentication method. This method is commonly used in Enterprise networks.

WPA Pre-shared Key: the pass phrase for WPA™ or WPA2™ security method should be specified if the *Pre-shared Key* method is selected. The pre-shared key is an alpha-numeric password between 8 and 63 characters long.

MAC ACL: MAC Access Control List (ACL) provides the ability to allow or deny certain clients to connect to the AP (applicable for AP and AP WDS modes only).

MAC ACL can be enabled by selecting the **Enabled** option.

There are two ways to set the Access Control List:

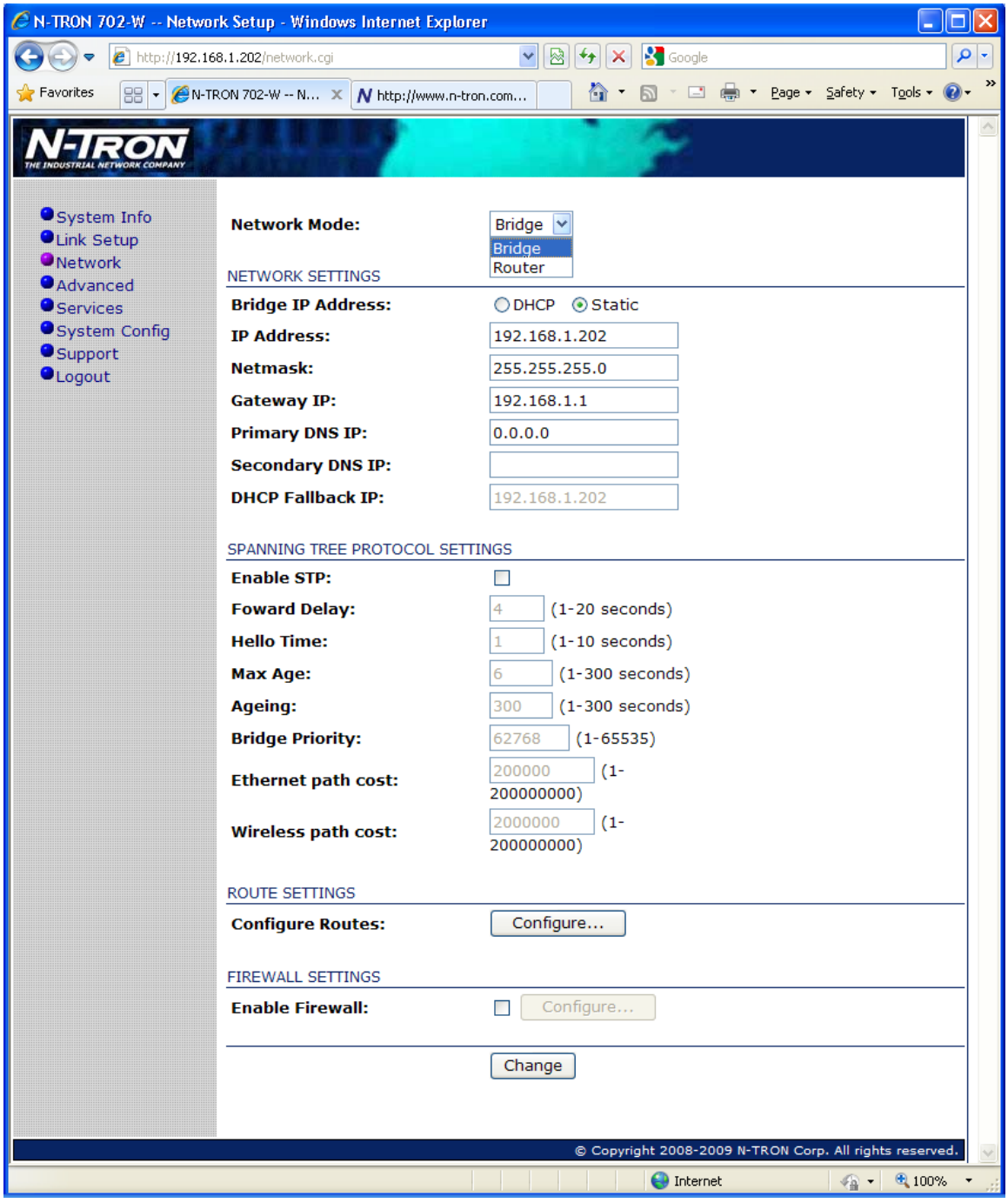
Define certain wireless clients in the list which will have granted access to the Access Point. Access will be denied for all remaining clients - MAC ACL **Policy** is set to *Allow*.
Define certain wireless clients in the list which will have denied access to the Access Point. Access will be granted for all remaining clients - MAC ACL **Policy** is set to Deny.

The MAC addresses of wireless clients can be added and removed to the list using the **Add** and **Remove** buttons.

Note: MAC Access Control is the weakest security approach. WPA™ or WPA2™ security methods should be used when possible.

Click **Change** button to save the changes.

Network Page



The Network Page allows the administrator to setup bridge or routing functionality.

N-TRON 702-W powered devices can operate in bridge or router mode. The IP configuration as described below is required for device management purposes. IP addresses can either be retrieved from a DHCP server or configured manually. Use the *Network* menu to configure IP settings.

Network Mode: specify the operating network mode for the device.

The mode depends on the network topology requirements:

Bridge operating mode is selected by default as it is widely used by subscriber stations, while connecting to Access Point or using WDS. In this mode the device will act as a transparent bridge and will operate in Layer 2. There will be no network segmentation while broadcast domain will be the same. Bridge mode will not block any broadcast or multicast traffic. Additional *Firewall* settings can be configured for Layer 2 packet filtering and access control in *Bridge* mode.
Router operating mode can be configured in order to operate in Layer 3 to perform routing and enable network segmentation. Wireless clients will be on a different IP subnet. **Router** mode will block broadcasts while it is not transparent.

N-TRON 702-W supports Multicast packet pass-through in **Router** mode.

N-TRON 702-W powered *Router* can act as a DHCP server and supports Network Address Translation (Masquerading) feature which is widely used by Access Points. NAT will act as the firewall between LAN and WLAN networks. Addition *Firewall* settings can be configured for Layer 3 packet filtering and access control in *Router* mode.

Bridge Mode

In bridge mode, the N-TRON 702-W will simply forward the network management and data packets to the client PC without any intelligent routing. For some applications, this can provide a more efficient and simple network solution. WLAN (wireless) and LAN (Ethernet) interfaces belong to the same network segment which has the same IP address space. WLAN and LAN interfaces form the virtual *bridge* interface while acting as *bridge* ports. The *bridge* has assigned IP settings for management purposes:

Bridge IP Address: The device can be set for static IP or can be set to obtain an IP address from the DHCP server connected to it.

One of the IP assignment modes must be selected:

DHCP – choose this option to assign the dynamic IP address, Gateway and DNS address by the local DHCP server.
Static – choose this option to assign static IP settings for the *bridge* interface.

IP Address: enter the IP address of the device while *Static Bridge IP Address* mode is selected. This IP will be used for the N-TRON 702-W device management purposes.

IP Address and *Netmask* settings should be consistent with the address space of the network segment where the 702-W resides. If the 702-W's and the administrator PC's (which is connected to the device on the wired or wireless interface) IP settings reside in different address spaces, the 702-W will become unreachable.

Netmask: This is a value which when expanded into binary provides a mapping to define which portions of the IP address groups can be classified as host devices and network devices. Netmask defines the address space of the network segment where N-TRON 702-W device resides. 255.255.255.0 (or /24) *Netmask* is commonly used among many C Class IP networks.

Gateway IP: Typically, this is the IP address of the host router which provides the point of connection to the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The 702-W will direct the packets of data to the gateway if the destination host is not within the local network.

Gateway IP address should be from the same address space (on the same network segment) as the N-TRON 702-W device.

Primary/Secondary DNS IP: The Domain Name System (DNS) is an Internet "phone book" which translates domain names to IP addresses. These fields identify the server IP addresses for the N-TRON 702-W device to look for the translation source.

Primary DNS server IP address should be specified for device management purposes.

Secondary DNS server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

DHCP Fallback IP: If the *Bridge* is placed in Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid DHCP server, it will fall back to this static IP address.

The N-TRON 702-W system will return to the default IP configuration (192.168.1.202/255.255.255.0) if the *Reset to defaults* routine is initiated.

Spanning Tree Protocol: Multiple interconnected bridges create larger networks using the IEEE 802.1d *Spanning Tree Protocol* (*STP*), which is used for finding the shortest path within the network and to eliminate loops from the topology.

If the *STP* is turned on, the N-TRON 702-W *Bridge* will communicate with other network devices by sending and receiving *Bridge Protocol Data Units* (BPDU). *STP* should be turned off (selected by default) when the N-TRON 702-W device is the only bridge on the LAN or when there are no loops in the topology as there is no sense for the *bridge* to participate in the *Spanning Tree Protocol* in this case. Note that STP is only supported with WEP encryption.

Click **Change** button to save the changes.

Router Mode

IP Address: This is the IP address to be represented by the wireless interface of the 702-W.

Netmask: This is used to define the host and device classification for the chosen IP address range. 255.255.255.0 is a typical value.

Enable NAT: Network Address Translation (NAT) enables packets to be sent from the outside world to the wireless interface IP address and then sub-routed to other client devices residing on its local network.

Enable DHCP Server: Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to clients who will associate to the wireless interface.

Range Start/End: This range will determine the IP addresses given out by the DHCP server to associated client devices.

Netmask: DHCP Netmask

Lease Time: The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensures client operation without interrupt, but could introduce potential

conflicts. Lowering the lease time will avoid potential address conflicts, but may cause slight interruptions to the client while re-acquiring a new IP addresses from the server.

Port Forwarding: Port forwarding allows specific ports of the WLAN IP address to be forwarded to different IP addresses on the same network. This is useful for applications such as FTP servers, HTTP servers, etc. where different host systems want to be seen using a single common IP address.

PPPoE: Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems which enables encapsulated data transport. It is commonly used as the medium for subscribers to connect to Internet Service Providers.

Enable DMZ: The Demilitarized zone (DMZ) can be used as a place where services can be placed such as Web Servers, Proxy Servers, and E-mail Servers such that these services can still serve the local network and are at the same time isolated from it for additional security.

MULITCAST ROUTING SETTINGS

With a multicast design, applications can send one copy of each packet and address it to the group of computers that want to receive it. This technique addresses packets to a group of receivers rather than to a single receiver, and is dependent on the network to forward the packets to only the networks that need to receive them.

Advanced Page

This page handles advanced routing and wireless settings. The Advanced options page allows you to manage advanced settings that influence the device performance and behavior. The advanced wireless settings are for more technically advanced users who have sufficient knowledge about wireless LAN technology. These settings should not be changed unless you know what effect the changes will have on your device.

Advanced Wireless Settings

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The valid range is 0-2347bytes, or “off”. The default value is 2347 which means RTS is disabled.

RTS/CTS (Request to Send / Clear to Send) is the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden terminal problem. RTS/CTS packet size threshold is 0-2347 octets. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake is triggered. If the packet size is equal to or less than threshold the data frame is sent immediately

Fragmentation Threshold: specifies the maximum size of a packet before data is fragmented into multiple packets. The valid range is 256-2346 bytes, or the word “off”. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended, the default setting of 2346 should remain in most cases.

The use of fragmentation can increase the reliability of frame transmissions. Because sending smaller frames, collisions are much less likely to occur. The fragment size should typically be set between 256 and 2,048 bytes.

Aggregation: Allows a much larger "burst" of frame data to be sent. Note: Aggregation will disable multicast traffic from crossing the radio link and may change the order in which packets are sent across the link (not recommended for controls networks) so it should only be used with a protocol that supports reordering of packets like TCP.

Enable Extra Reporting: Un-check this if you are having problems with Intel Chipset wireless cards

Enable Client Isolation: This option allows packets only to be sent from the router to the CPE. In other words, CPE's on the same network as the AP will not be able to see each other.

Acknowledgment Timeout

N-TRON 702-W has an auto-acknowledgment timeout algorithm which dynamically optimizes the acknowledgment timeout value without user intervention. This is a critical feature required for stabilizing long-distance outdoor links. The user has the ability to enter the value manually, but this is not recommended.

Distance: specify the distance value in miles using slider or enter the value manually. The signal strength and throughput falls off with range. Changing the distance value will change the ACK Timeout to the appropriate value of the distance. The ACK timeout is calculated in microseconds and should take into consideration the round trip flight time over the air.

ACK Timeout: specify the ACK Timeout. This is the amount of time the subscriber station will wait to hear an acknowledgment response from the wireless device after the data packet is transmitted. If the timeout is set too short or too long, it will result in poor connection and throughput performance.

Changing the ACK Timeout value will change the Distance to the appropriate distance value for the ACK Timeout.

The Auto Adjust control will enable the ACK Timeout Self-Configuration feature. If enabled, the ACK Timeout value will be derived dynamically using an algorithm similar to the Conservative Rate Algorithm described above.

Antenna Alignment LED Thresholds

The LED's on the 702-W can turn on the LED when received signal levels reach the values defined in the following fields. This allows a technician to easily deploy an N-TRON 702-W CPE without logging into the unit.

LED 1 (Green) will switch on if the dBm reach the set value (Default = -30dBm).

LED 2 (Green) will switch on if the dBm reach the set value (Default = -60dBm).

LED 3 (Orange) will switch on if the dBm reach the set value (Default = -70dBm).

LED 4 (Red) will switch on if the dBm reach the set value (Default = -90dBm).

Only 1 LED will light at a given moment in time to show signal level in the order above.

EX: Power Received = -46dBm
LED Configuration:

LED1	LED2	LED3	LED4
-40dBm	-50dBm	-60dBm	-70dBm

In this situation LED2 will be illuminated because the signal is worse then the threshold of LED1 and better than the threshold of LED2.

Wireless Traffic Shaping

Wireless Traffic shaping feature is dedicated for upstream and downstream bandwidth control while looking from the client (connected on Ethernet interface) perspective.

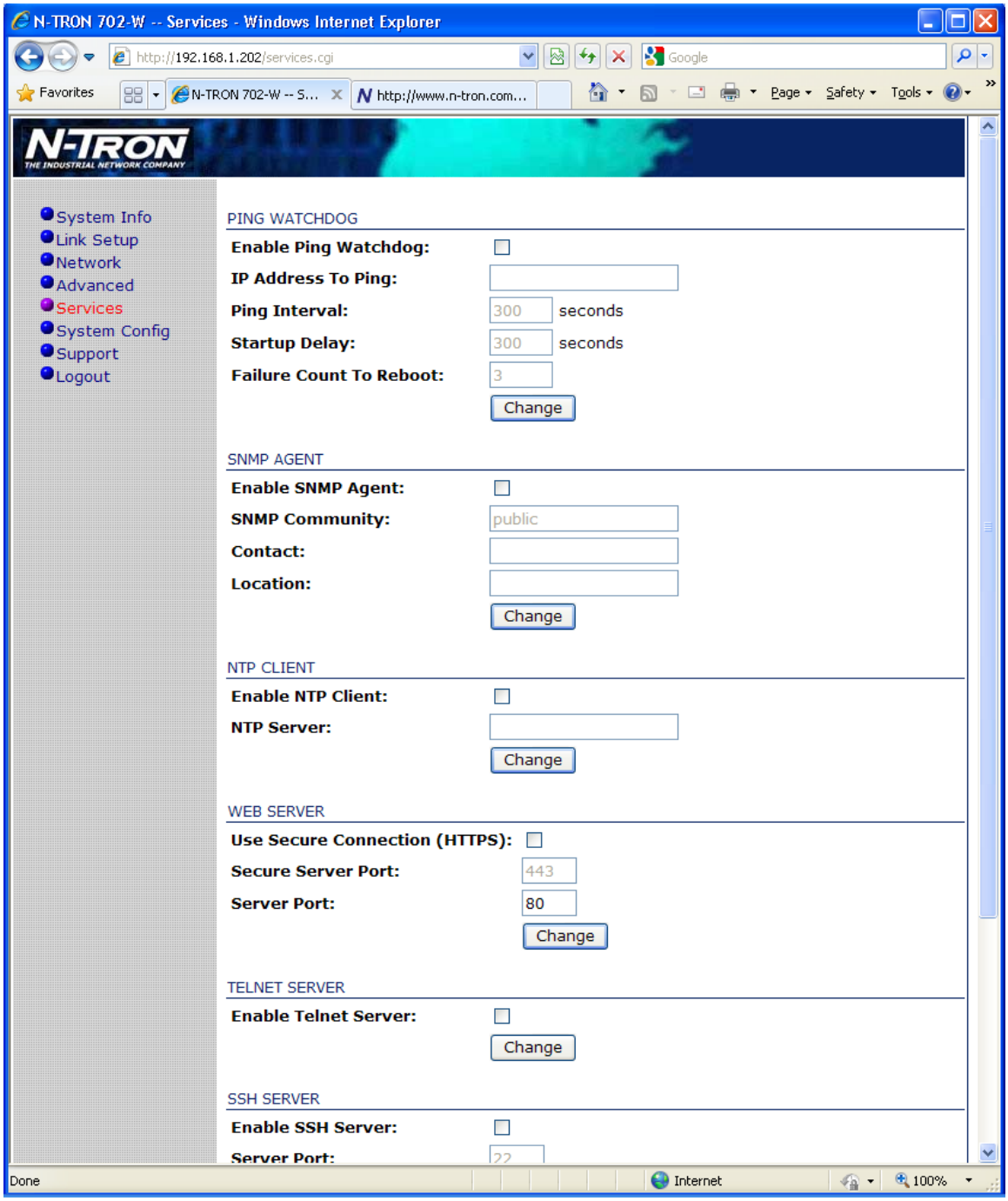
Traffic Shaping: The traffic can be limited by the N-TRON 702-W in the upload and download direction based on a user defined rate limit for each direction.

Enable Traffic Shaping: control will enable bandwidth control on the device.

Incoming Traffic Limit: specify the maximum bandwidth in kbps for traffic passing from the wireless interface to the Ethernet interface.

Outgoing Traffic Limit: specify the maximum bandwidth in kbps for traffic passing from the Ethernet interface to the wireless interface.

Service Page



This page covers the configuration of the following system management services; Ping Watchdog, SNMP, NTP, Web Server, Telnet Server, SSH Server and System Log.

Ping WatchDog

The ping watchdog sets the N-TRON 702-W Device to continuously ping a user defined IP address (for example the Internet gateway). If it is unable to ping under the user defined constraints, the N-TRON 702-W device will automatically reboot. This option decreases the likelihood of failure using a relative "fail-proof" mechanism.

Ping Watchdog is dedicated for continuous monitoring of a particular connection to a remote host using the Ping tool. Ping works by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. If the defined number of replies is not received, the tool reboots the device.

Enable Ping Watchdog: control will enable the Ping Watchdog Tool.

IP Address To Ping: specify an IP address of the target host which will be monitored by the Ping Watchdog Tool.

Ping Interval: specify a time interval (in seconds) between the ICMP “echo requests” sent by the Ping Watchdog Tool.

Startup Delay: specify initial time delay (in seconds) until the first ICMP “echo requests” are sent by the Ping Watchdog Tool. The value of the Startup Delay should be at least 60 seconds as the network interface and wireless connection initialization takes a considerable amount of time if the device is rebooted.

Failure Count To Reboot: specify the number of ICMP “echo response” replies. If the specified number of ICMP “echo response” packets is not received continuously, the Ping Watchdog Tool will reboot the device.

SNMP Agent

Simple Network Monitor Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. The N-TRON 702-W contains an SNMP agent which allows it to communicate to SNMP managed applications for network provisioning.

The SNMP Agent provides an interface for device monitoring using the Simple Network Management Protocol (an application layer protocol that facilitates the exchange of management information between network devices). The SNMP Agent allows network administrators to monitor network performance, find and troubleshoot network problems. For the purpose of equipment identification, it is always a good idea to configure SNMP agents with contact and location information:

Enable SNMP Agent: control will enable the SNMP Agent.

SNMP Community: specify SNMP community string. It is required to authenticate access to MIB objects and functions as embedded password. The device supports a Read-only community string that gives read access to authorized management stations of all objects in the MIB except community strings, write access is not allowed.

Contact: specify the identity or the contact for notification of emergency situations.

Location: specify the physical location of the device.

NTP Client, Web Server, Telnet Server

NTP Client: The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It can be used to set the N-TRON 702-W internal clock.

Web Server: the following N-TRON 702-W Device Web Server parameters can be set:

Use Secure Connection (HTTPS): If checked Web server will use secure HTTPS mode. HTTP mode is selected by default.

Secure Server Port: Web Server TCP/IP port setting while using HTTPS mode.

Server Port: Web Server TCP/IP port setting while using HTTP mode.

Telnet Server: the following N-TRON 702-W Device Telnet Server parameters can be set:

Enable Telnet Server: Enables Telnet access to the N-TRON 702-W Device.

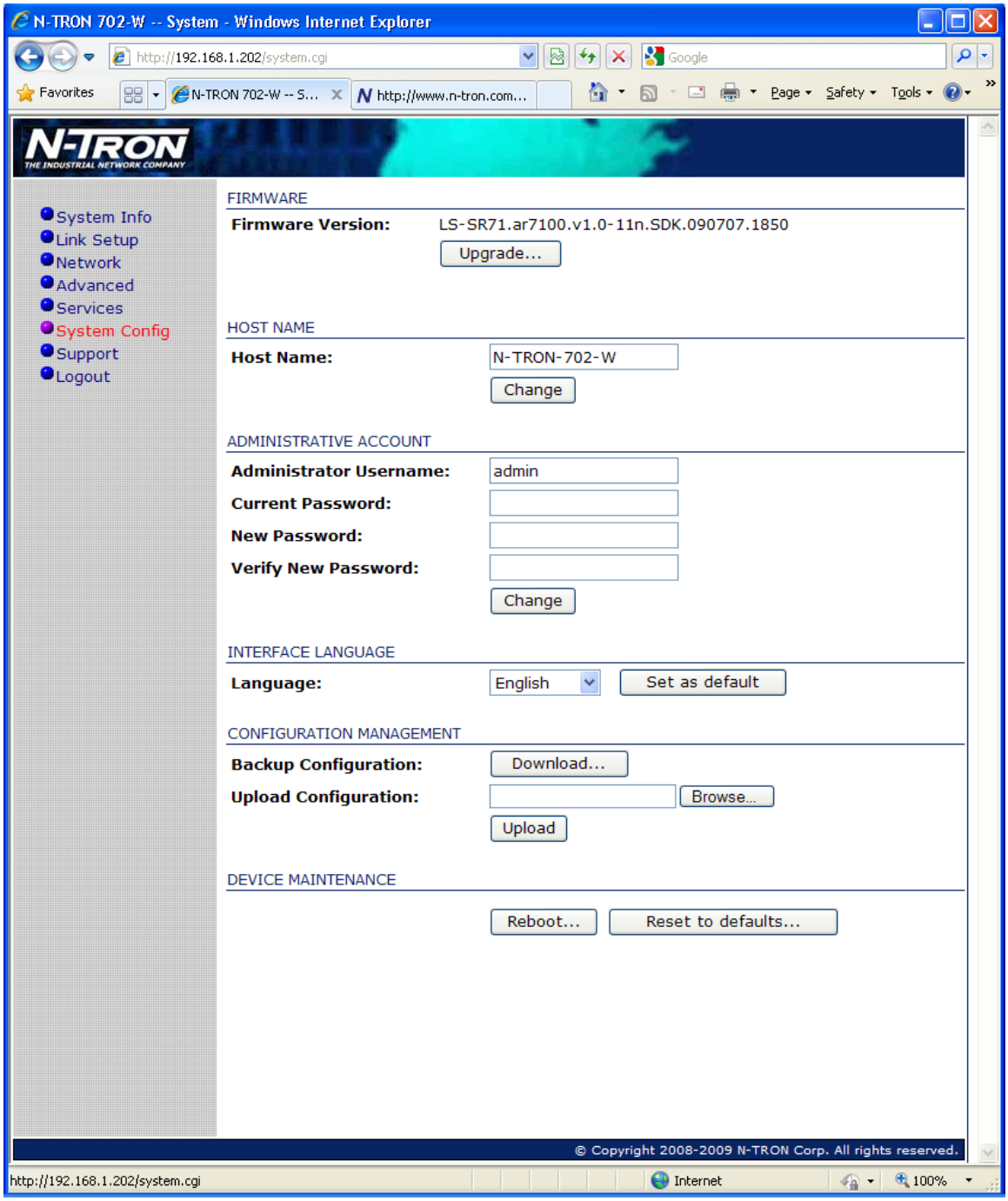
Server Port: Telnet service TCP/IP port setting.

System Log: Logs system information locally and/or to a remote logging server.

Enable Log: Enables local logging for the device.

Enable Remote Log: Enables remote logging to a specified logging server.

System Config Page



The System Config Page contains Administrative options. This page enables administrator to reboot the device, set it to factory defaults, upload new firmware, backup or update the configuration and establish administrator's credentials.

Firmware

Use this section to find out current software version and update the device with new firmware. The device firmware update preserves all configuration settings. When the device is updated with a newer version or the same version firmware builds, system configuration will be preserved.

Firmware version: displays version of the current firmware.

Upgrade…: click to load the device firmware upgrade window. After the Upgrade… button is clicked the new Firmware Upload pop-up window will be displayed:

> **Current Firmware**: displays version of the current firmware. Firmware File: click the Browse… button to specify the new firmware image location or specify the full path and click the Upload button. Close this window – cancel the upload process. After the new firmware image is uploaded into the system, use Upgrade button to upgrade a device:

Do not switch off, do not reboot and do not disconnect the device from the power supply during the firmware upgrade process as this can damage the device!

After clicking the Upgrade button the upgrade process starts immediately:

Close this window – closes the firmware upgrade window. This action will not cancel the firmware upgrade process, but will try to load the web page before the unit is ready and may result in a page can't be displayed error.

Host Name

Host Name is the system wide device identifier. It is reported by the SNMP Agent to authorized management stations.

Host Name: specify the system identity. Click the Change button to save the changes.

Administrative Account

In this section you can modify the administrator password to protect your device from unauthorized configuration. The default administrator's password should be changed on the very first setup:

Administrator Username: displays name of the system user.

Current Password: enter a current password value.

Default administrator login credentials:

User Name: admin

Password: admin

New Password: enter a new password value used for administrator authentication.

Verify Password: re-enter the new password to verify its accuracy.

Note: Click **Change** button to save the changes.

Interface Language

Use this section to change the language setting of the web management interface.

Configuration Management

Use the Configuration Management section controls to manage (backup, restore/update) the system configuration file:

Backup Configuration: click the Download… button to download the current system configuration file.

Upload Configuration: click the Browse… button to navigate to and select the new configuration file or specify the full path and click the Upload button.

Device Maintenance

Use this section to reboot device or reset all system parameters to factory default values:

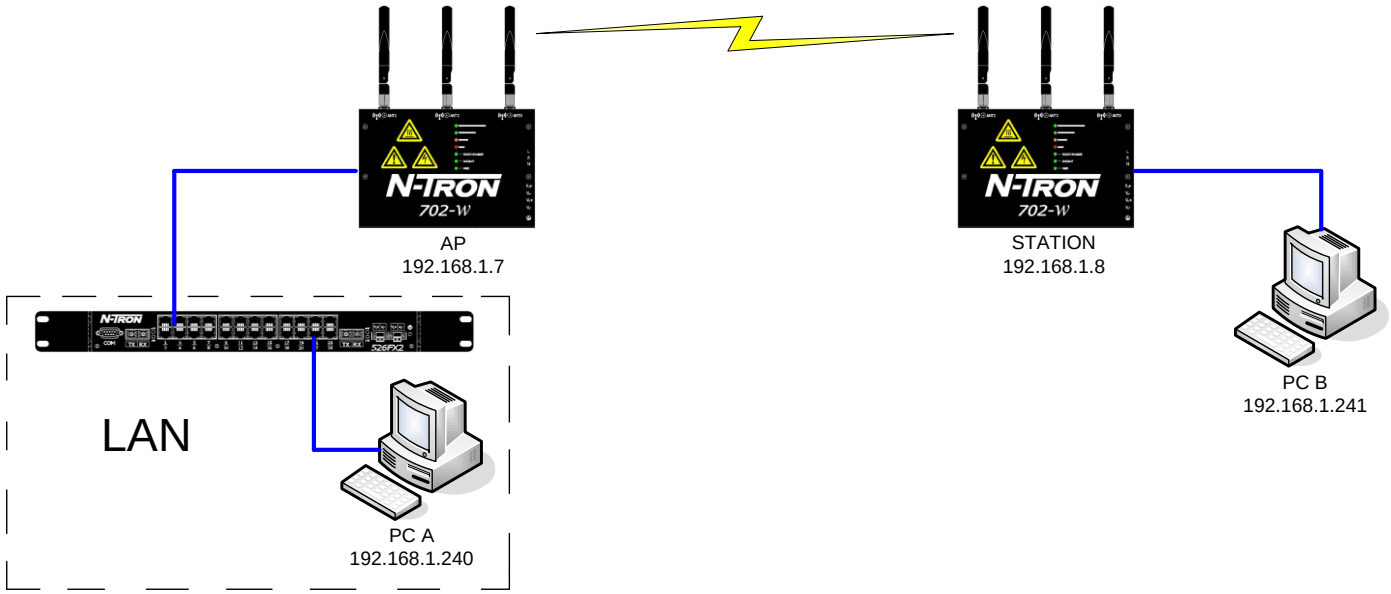
Reboot: click to reboot the device in the current configuration. Any non-applied changes will be lost.

Reset to Defaults: click to reset the device to factory defaults.

Common Topology Scenarios

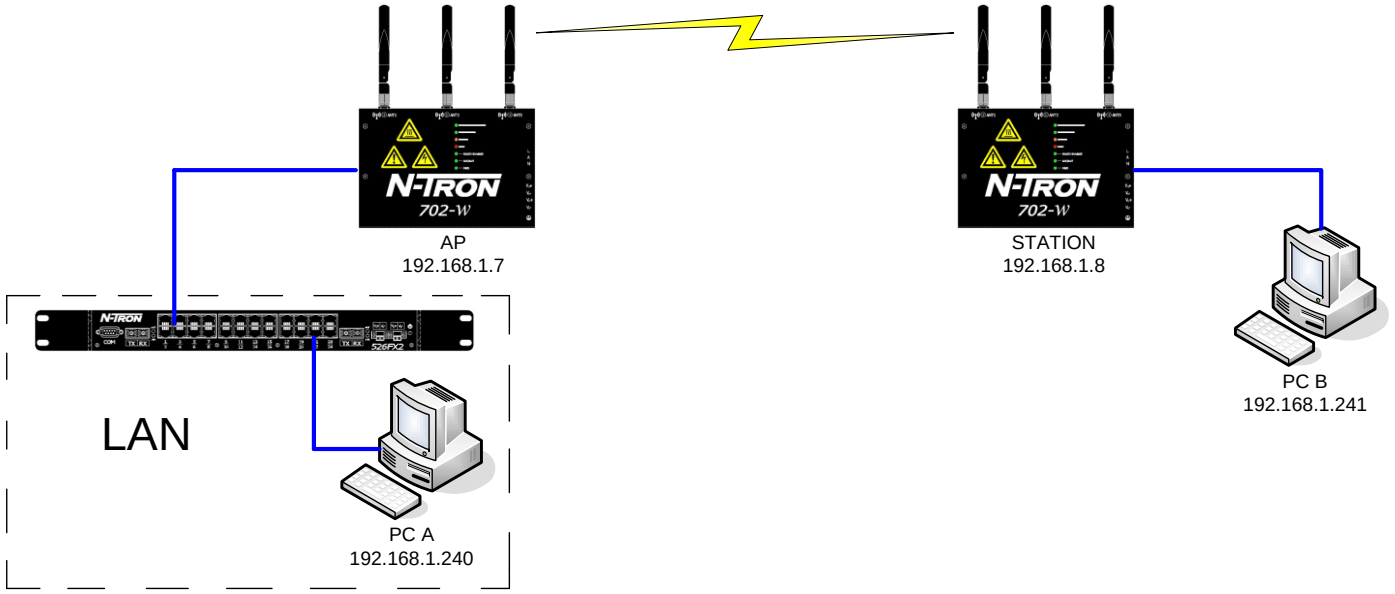
The goal of this section is to provide a foundation of how reliable wireless network typologies should be designed. It is not intended as a cookie cutter solution for installing wireless networks.

Scenario 1 – Basic Bridge



Link Setup:		Link Setup:	
	Wireless Mode: AP		Wireless Mode: Station
	SSID: N-Tron		ESSID: N-Tron
	Country Code: United States		Country Code: United States
	802.11 Mode: 11Ng-20MHz		802.11 Mode: 11Ng-20MHz
	Channel: 10 – 2457MHz		Extension Channel: N/A
	Extension Channel: N/A		Output Power: 12dBm
	Output Power: 12dBm		
Network:		Network:	
	Mode: Bridge		Mode: Bridge
	IP Address: 192.168.1.7		IP Address: 192.168.1.8
	Netmask: 255.255.255.0		Netmask: 255.255.255.0
	Gateway: 192.168.1.1		Gateway: 192.168.1.1

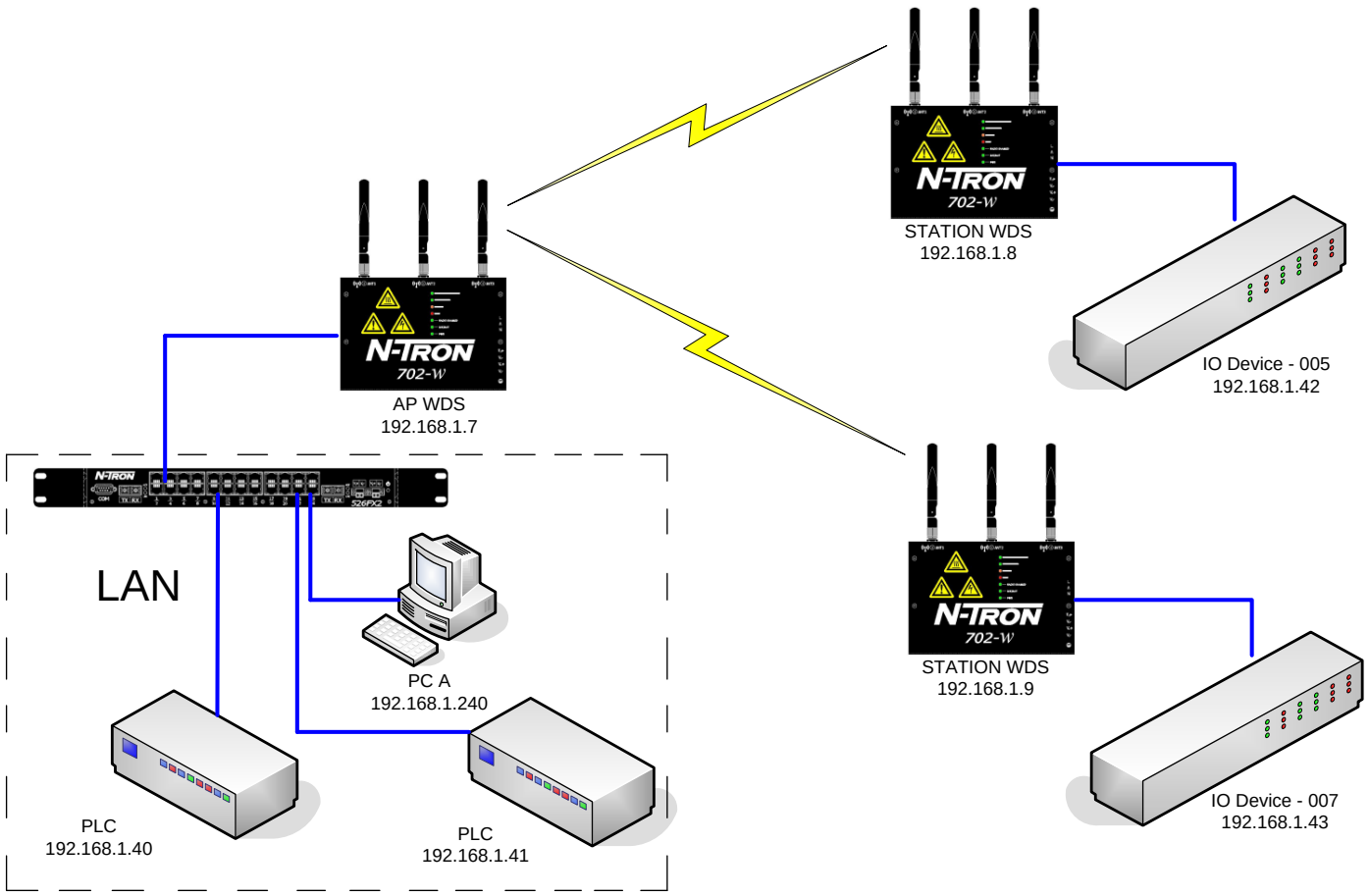
Scenario 2 – Encrypted Bridge



Link Setup:	
Wireless Mode:	AP
SSID:	N-Tron
Country Code:	United States
802.11 Mode:	11Ng-20MHz
Channel:	10 – 2457MHz
Extension Channel:	N/A
Output Power:	12dBm
Security:	WPA2-AES
WPA Preshared key:	ntron001
Network:	
Mode:	Bridge
IP Address:	192.168.1.7
Netmask:	255.255.255.0
Gateway:	192.168.1.1

Link Setup:	
Wireless Mode:	Station
ESSID:	N-Tron
Country Code:	United States
802.11 Mode:	11Ng-20MHz
Extension Channel:	N/A
Output Power:	12dBm
Security:	WPA2-AES
WPA Preshared key:	ntron001
Network:	
Mode:	Bridge
IP Address:	192.168.1.8
Netmask:	255.255.255.0
Gateway:	192.168.1.1

Scenario 3 – Controls Network

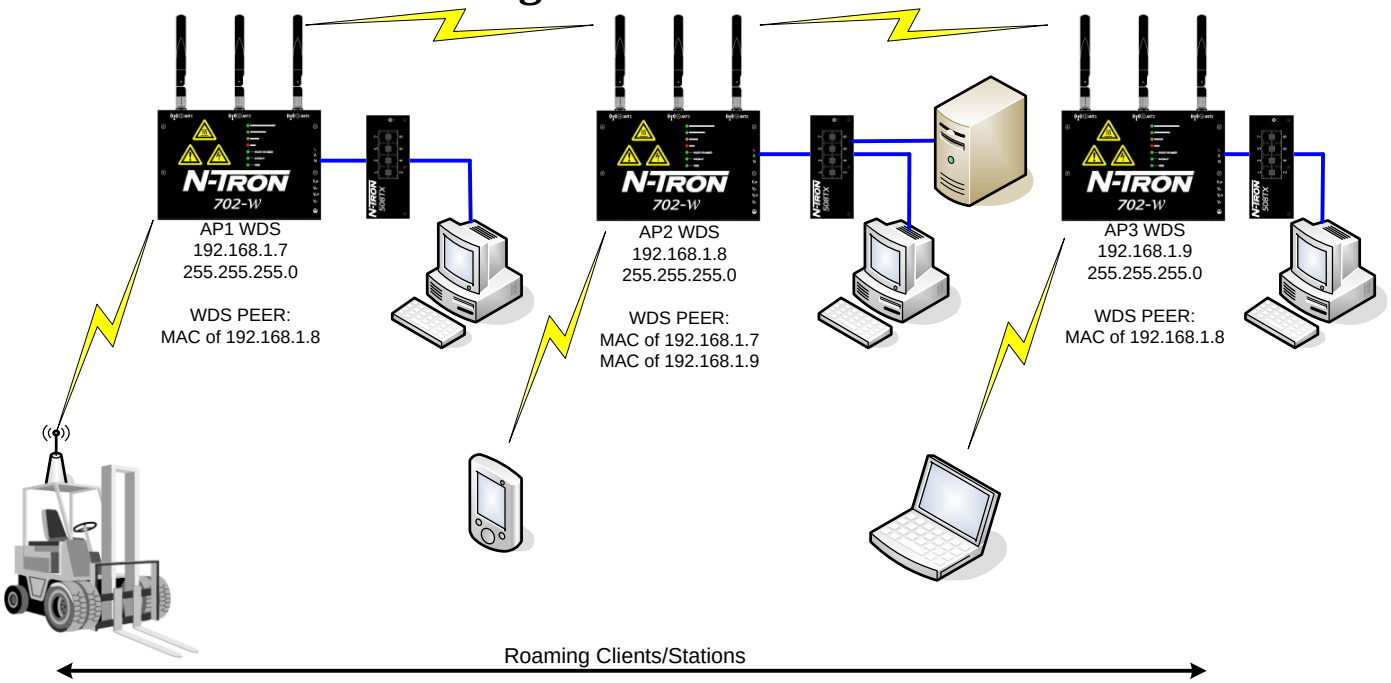


Link Setup:	
Wireless Mode:	AP WDS
SSID:	N-Tron
Country Code:	United States
802.11 Mode:	11Ng-40MHz
Channel:	10 – 2457MHz
Extension Channel:	N/A
Output Power:	12dBm
Network:	
Mode:	Bridge
IP Address:	192.168.1.7
Netmask:	255.255.255.0
Gateway:	192.168.1.1

Link Setup:	
Wireless Mode:	Station WDS
ESSID:	N-Tron
Country Code:	United States
802.11 Mode:	11Ng-40MHz
Extension Channel:	N/A
Output Power:	12dBm
Network:	
Mode:	Bridge
IP Address:	192.168.1.8
Netmask:	255.255.255.0
Gateway:	192.168.1.1

Link Setup:	
Wireless Mode:	Station WDS
ESSID:	N-Tron
Country Code:	United States
802.11 Mode:	11Ng-40MHz
Extension Channel:	N/A
Output Power:	12dBm
Network:	
Mode:	Bridge
IP Address:	192.168.1.9
Netmask:	255.255.255.0
Gateway:	192.168.1.1

Scenario 4 – WDS Peering

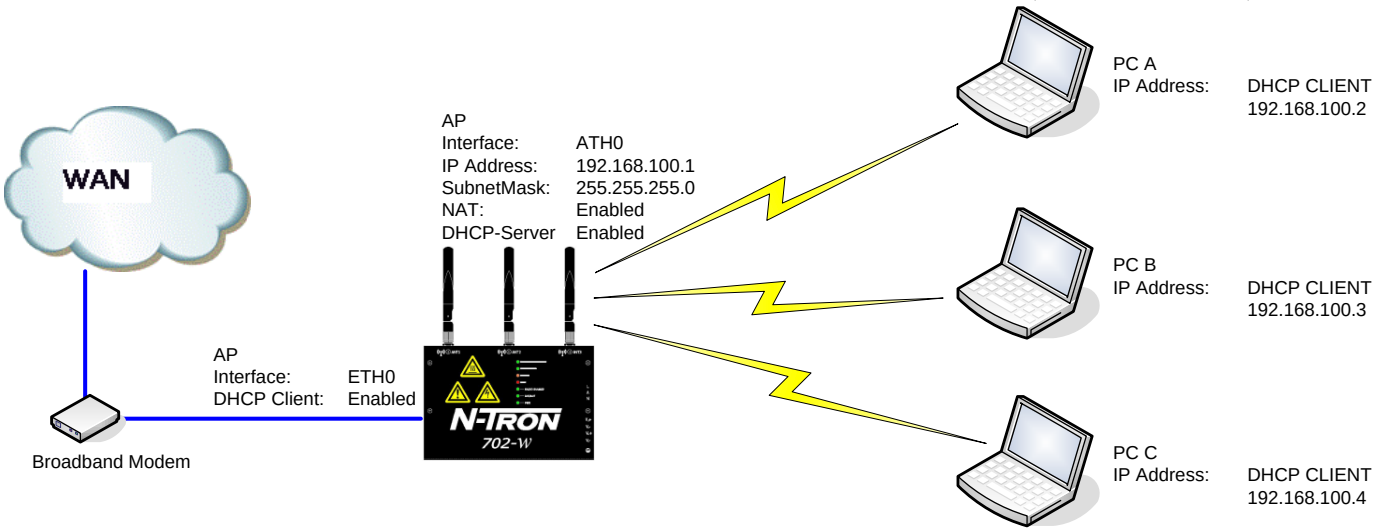


AP1	
Link Setup:	
Wireless Mode:	AP WDS
SSID:	N-Tron
WDS PEERS:	WLAN MAC AP2
Country Code:	United States
802.11 Mode:	11Ng-40MHz
Channel:	10 – 2457MHz
Extension Channel:	N/A
Output Power:	12dBm
Network:	
Mode:	Bridge
IP Address:	192.168.1.7
Netmask:	255.255.255.0
Gateway:	192.168.1.1

AP2	
Link Setup:	
Wireless Mode:	AP WDS
SSID:	N-Tron
WDS PEERS:	WLAN MAC AP1 WLAN MAC AP3
Country Code:	United States
802.11 Mode:	11Ng-40MHz
Channel:	10 – 2457MHz
Extension Channel:	N/A
Output Power:	12dBm
Network:	
Mode:	Bridge
IP Address:	192.168.1.8
Netmask:	255.255.255.0
Gateway:	192.168.1.1

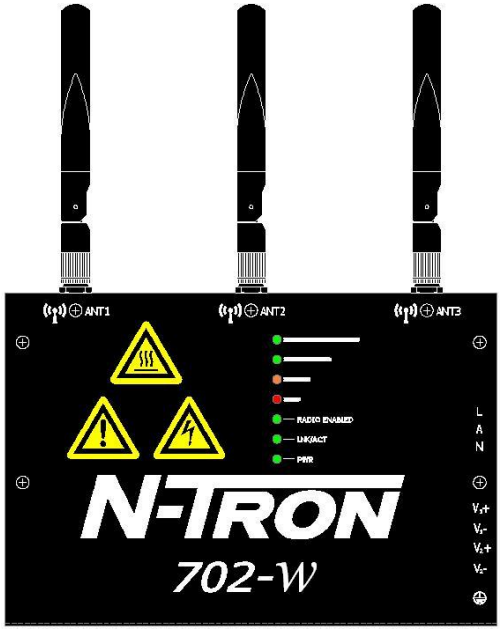
AP3	
Link Setup:	
Wireless Mode:	AP WDS
SSID:	N-Tron
WDS PEERS:	WLAN MAC AP2
Country Code:	United States
802.11 Mode:	11Ng-40MHz
Channel:	10 – 2457MHz
Extension Channel:	N/A
Output Power:	12dBm
Network:	
Mode:	Bridge
IP Address:	192.168.1.9
Netmask:	255.255.255.0
Gateway:	192.168.1.1

Scenario 5 – Broadband Modem Wireless Router (W/ DHCP)



Link Setup:	
Wireless Mode:	AP
SSID:	N-Tron
Country Code:	United States
802.11 Mode:	11Ng-20MHz
Channel:	10 – 2457MHz
Extension Channel:	N/A
Output Power:	12dBm
Network:	
Mode:	Router
WLAN:	
IP Address:	192.168.100.1
Netmask:	255.255.255.0
NAT:	Enabled
DHCP-Server:	Enabled
Start Range:	192.168.100.2
End Range:	192.168.100.30
LAN:	
DHCP Client:	Enabled

702-W Key Specifications



Switch Properties

Number of MAC Addresses:	10,000
Number of IP Addresses:	1024
MAC Aging Time:	300 seconds
ARP Aging Time:	60 seconds
Latency (Typical):	< 1ms
Switching Method:	Store & Forward

Physical

Height: (w/o antennas)	4.75" / 12.065 cm
Width:	7.0" / 17.78 cm
Depth: (w/ DIN-Rail CLIP)	1.17" / 2.9718 cm
Weight (max):	1.9 lbs / 0.86kg
Din-Rail mount:	35mm

Electrical

Redundant Input Voltage:	20-49VDC (Regulated)
702-W Input Current (max):	200mA max. @ 24VDC
702-W Max Power:	4.8Watts max
Input Ripple:	Less than 100 mV
N-TRON Power Supply:	NTPS-24-1.3 (1.3 Amp@24VDC*)* (NOTE: Not appropriate for use with M12, POE, and HV models.)

Environmental

Operating Temperature: -40°C to 70°C
Storage Temperature: -40°C to 85°C

Operating Humidity: 5% to 95% (Non Condensing)

Operating Altitude 0 to 10,000 ft.

Reliability

MTBF: >1 Million Hours

Connectors

10/100BaseTX: (1) RJ-45 Copper Port (w/ PoE Support)
802.11abgn: (3) RP-SMA Connectors

Recommended Wiring Clearance:

Side: 4" (10.16 cm)
Top: 6" (15.24 cm) – Dependent on antenna

Network Media

10BaseT: >Cat3 Cable
100BaseTX: >Cat5 Cable
minimum length : 1 meter
maximum length : 100 meters

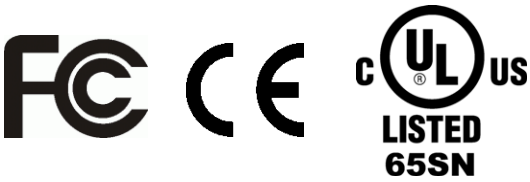
Warranty: 3 years from the date of purchase.

Regulatory Approvals:

SAFETY: UL listed per ANSI/ISA-12.12.01-2007 (US and Canada)
This equipment is suitable for use in Class I, Div 2, Groups A, B, C, and D or non-hazardous locations only.

FCC (EMI): ANSI C63.4-2003: Radio-Noise Emissions
US CFR 47, Part 15, Subpart B, Unintentional Radiators
Industry Canada ICES-003 Issue 3: Digital Apparatus

CE (EMC): EN 61000-4-2 Ed. 1.2 (Electrostatic Discharge)
EN 61000-4-3 3rd Ed. (Radio-frequency Electromagnetic Field Amplitude Modulated)
EN 301 489-3 V1.4.1 (Radiated Emissions)



702M12-W Key Specifications

Switch Properties

Number of MAC Addresses:	10,000
Number of IP Addresses:	1024
MAC Aging Time:	300 seconds
ARP Aging Time:	60 seconds
Latency (Typical):	< 1ms
Switching Method:	Store & Forward

Physical

Height: (w/o antennas)	6.62" / 16.81 cm
Width:	6.62" / 16.81 cm
Depth:	1.71" / 4.34 cm
Weight (max):	3.5 lbs / 1.54kg
Din-Rail mount:	35mm (optional)

Electrical

Redundant Input Voltage:	20-49VDC (Regulated)
702-W Input Current (max):	200mA max. @ 24VDC
702-W Max Power:	4.8Watts max
Input Ripple:	Less than 100 mV
N-TRON Power Supply:	NTPS-24-1.3 (1.3 Amp@24VDC*)* (NOTE: Not appropriate for use with M12, POE, and HV models.)

Environmental

Operating Temperature: -40°C to 70°C
Storage Temperature: -40°C to 85°C

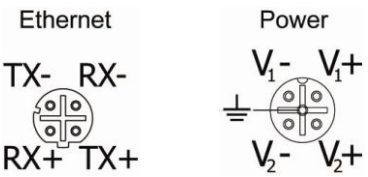
Operating Humidity: 5% to 100% (Non Condensing)

Operating Altitude 0 to 10,000 ft.

Reliability

MTBF: > 1 Million Hours

Pin Assignments:



Connectors

10/100BaseTX: (1) M12 D-Coded Port (w/ PoE Support)
802.11abgn: (3) RP-TNC Connectors
Power: (1) M12 A-Coded Port

Recommended Wiring Clearance:

Front: 6" (15.24 cm) – Dependent on antenna

Network Media

10BaseT: >Cat3 Cable
100BaseTX: >Cat5 Cable
minimum length : 1 meter
maximum length : 100 meters

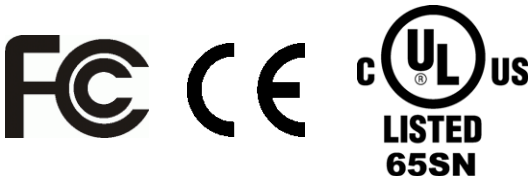
Warranty: 3 years from the date of purchase.

Regulatory Approvals:

SAFETY: UL listed per ANSI/ISA-12.12.01-2007 (US and Canada)
This equipment is suitable for use in Class I, Div 2, Groups A, B, C, and D or non-hazardous locations only.

FCC (EMI): ANSI C63.4-2003: Radio-Noise Emissions
US CFR 47, Part 15, Subpart B, Unintentional Radiators
Industry Canada ICES-003 Issue 3: Digital Apparatus

CE (EMC): EN 61000-4-2 Ed. 1.2 (Electrostatic Discharge)
EN 61000-4-3 3rd Ed. (Radio-frequency Electromagnetic Field Amplitude Modulated)
EN 301 489-3 V1.4.1 (Radiated Emissions)



N-TRON Limited Warranty

N-TRON, Corp. warrants to the end user that this hardware product will be free from defects in workmanship and materials, under normal use and service, for the applicable warranty period from the date of purchase from N-TRON or its authorized reseller. If a product does not operate as warranted during the applicable warranty period, N-TRON shall, at its option and expense, repair the defective product or part, deliver to customer an equivalent product or part to replace the defective item, or refund to customer the purchase price paid for the defective product. All products that are replaced will become the property of N-TRON. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer. N-TRON shall not be responsible for any custom software or firmware, configuration information, or memory data of customer contained in, stored on, or integrated with any products returned to N-TRON pursuant to any warranty.

OBTAINING WARRANTY SERVICE: Customer must contact N-TRON within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from N-TRON or its authorized reseller may be required. Products returned to N-TRON must be pre-authorized by N-TRON with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment. Responsibility for loss or damage does not transfer to N-TRON until the returned item is received by N-TRON. The repaired or replaced item will be shipped to the customer, at N-TRON's expense, not later than thirty (30) days after N-TRON receives the product. N-TRON shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to N-TRON for repair, whether under warranty or not.

ADVANCE REPLACEMENT OPTION: Upon registration, this product qualifies for advance replacement. A replacement product will be shipped within three (3) days after verification by N-TRON that the product is considered defective. The shipment of advance replacement products is subject to local legal requirements and may not be available in all locations. When an advance replacement is provided and customer fails to return the original product to N-TRON within fifteen (15) days after shipment of the replacement, N-TRON will charge customer for the replacement product, at list price.

WARRANTIES EXCLUSIVE: IF AN N-TRON PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT N-TRON'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. N-TRON NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. N-TRON SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, POWER CUTS OR OUTAGES, OTHER HAZARDS, OR ACTS OF GOD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW, N-TRON ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF N-TRON OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT N-TRON'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

DISCLAIMER: Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

GOVERNING LAW: This Limited Warranty shall be governed by the laws of the State of Delaware, U.S.A